# CAIIB 2026

# Information Technology & Digital Banking

## CHAPTERWISE MCQ BANK

NODIA

Nodia

Scan QR for Demo PDF

# GET ALL STUDY MATERIAL IN ONE APP!

- Textbooks
- Previous Year Chapterwise Question Banks
- 30 Sets Sample Papers
- Worksheets

**FREE!**

## DOWNLOAD NOW!

**SCAN & DOWNLOAD**

GET IT ON Google Play

# CAIIB EXAMINATION 2026

# Information Technology & Digital Banking

## Chapterwise MCQ Bank

**NODIA**

Downloaded from www.pdf.tube

CAIIB Information Technology and Digital Banking
Edition May 2026
Published by :NODIA
An Imprint of NODIA EDITIONS LLP

Information contained in this book has been obtained by author, from sources believes to be reliable. However, neither NODIA nor its author guarantee the accuracy or completeness of any information herein and NODIA nor its author shall be responsible for any error, omissions, or damages arising out of use of this information. This book is published with the understanding that NODIA and its author are supplying information but are not attempting to render engineering or other professional services.

NODIA

© NODIA EDITIONS LLP

**MRP ₹690.00**

available at amazon

This book is available on amazon and flipkart only and not available in market.

**NODIA EDITIONS LLP**
125, Sector 6, Vidyadhar Nagar, Jaipur 302039
Phone :+91 9001005245
email : mail@nodia.in

# DISCLAIMER

- This book has been prepared on the basis of previous CAIIB examination questions, conceptual patterns, and memory-based feedback received from examination candidates. It is intended solely for academic practice and examination preparation purposes.
- The content provided herein is not an exact reproduction of any official CAIIB examination paper. Several questions have been revised, updated, modified, or restructured to align with the latest syllabus, examination pattern, banking developments, and evolving examination trends.
- In certain cases, questions may carry an examination year tag from an earlier year even though the factual context, numerical values, regulatory references, or examples may relate to a later period. Such tagging indicates the original conceptual source of the question and not necessarily the timeframe of the updated content.
- Questions marked as "Old Exam" are included only to indicate their historical conceptual origin and have been suitably revised wherever required to maintain consistency with the current CAIIB syllabus and examination framework.
- Some questions included in this book may not have appeared exactly in previous examinations; however, they are based on similar concepts, emerging trends, model patterns, and analytical approaches relevant to the CAIIB examination. Their inclusion is intended to strengthen conceptual clarity and improve examination readiness.
- As a portion of the material is based on memory-based feedback from candidates, minor variations in wording, structure, sequence, or presentation from the actual examination questions may exist.
- All tables, graphs, charts, figures, diagrams, and illustrative references mentioned in this book are derived from or inspired by the official study materials and recommended references prescribed by Indian Institute of Banking & Finance. Readers are advised to refer to the official publications for authoritative explanations, original illustrations, and complete details.
- This book is intended purely as a supplementary study aid and should not be considered a substitute for official study materials issued by Indian Institute of Banking & Finance. No claim is made regarding any association with, endorsement by, or authorization from Indian Institute of Banking & Finance.
- The examination syllabus, pattern, regulatory references, and guidelines are subject to change at the discretion of the examining body and relevant authorities. The publisher and authors shall not be held responsible for any errors, omissions, interpretation differences, or changes introduced after publication.
- The inclusion of questions, concepts, or practice material in this book does not guarantee success in the examination. Examination performance ultimately depends upon the individual's preparation, understanding, and application of concepts.

Click Here to Buy book on Amazon

# CONTENTS


| | | |
|---|---|---|
| CHAP 1. | Information Technology and Its Implications | 5 |
| CHAP 2. | Introduction to Computing Systems | 38 |
| CHAP 3. | Introduction to Software | 75 |
| CHAP 4. | Networking Systems | 109 |
| CHAP 5. | Introduction to Information Systems | 142 |
| CHAP 6. | Database Management Systems | 180 |
| CHAP 7. | Data Warehousing and Data Mining | 210 |
| CHAP 8. | E-Learning Environment | 243 |
| CHAP 9. | Banking Software | 277 |
| CHAP 10. | Electronic Clearing and Settlement Systems | 310 |
| CHAP 11. | Plastic Money | 345 |
| CHAP 12. | E-Commerce and E-Banking | 379 |
| CHAP 13. | IT Act 2000 - 2008 | 412 |
| CHAP 14. | Emerging Technologies | 445 |
| CHAP 15. | Computer Security | 479 |
| CHAP 16. | Communication Security | 512 |
| CHAP 17. | Business Continuity & Disaster Recovery Planning | 545 |
| CHAP 18. | Information System Audit | 580 |
| CHAP 19. | Competitive Bid Process: RFP and SLA | 613 |
| CHAP 20. | RBI Guidelines on Cyber Security & Digital Payment Security | 647 |


NODIA

**********

# CHAPTER 01

# Information Technology and Its Implications

May/June 2023

**1.** What is the expected global number of connected IoT devices by 2025?
(A) 12.3 billion
(B) 15 billion
(C) 150 million
(D) 27 billion

Oct/Nov 2008

**2.** How will the 'smart houses' of the future enhance comfort and security?
(A) By requiring manual adjustment of home heating systems
(B) By eliminating the need for any cyberspace connections
(C) By automating garden maintenance and visitor screening
(D) By forcing residents to work from their homes exclusively

May/June 2014

**3.** What does the acronym EASE stand for in the context of public sector banks?
(A) Electronic Access and System Effectiveness
(B) Enterprise Architecture and Security Evaluation
(C) Enhanced Access and Service Excellence
(D) Economic Assessment and System Efficiency

Oct/Nov 2021

**4.** Which statement represents the impact of the Government of India's demonetization initiative?
(A) It immediately eliminated all cash transactions in the economy.
(B) It proved to be a curse for India's e-payment providers.
(C) It, coupled with the COVID-19 pandemic, contributed to a multi-fold increase in digital transactions.
(D) It resulted in India handling only 2% of global real-time digital payments.

May/June 2005

**5.** Why are financial institutions focusing on converting from a service to a sales culture?
(A) Because traditional services have become completely obsolete
(B) Because retaining existing customers is more cost-effective
(C) Because acquiring new customers is easier than retention
(D) Because sales cultures require less information technology

Oct/Nov 2014

**6.** Which statement regarding business drivers for IT change is correct?
(A) Consumer behaviour shows a growing demand for service convenience and availability around the clock.
(B) There is decreasing pressure from shareholders for financial performance.
(C) Financial institutions are experiencing a decrease in competition.
(D) Large institutions are avoiding operational consolidation in the global market.

May/June 2021

**7.** What is a Neo-bank?
(A) A conventional bank using computerized banking programs
(B) An online bank without traditional physical branch networks
(C) A traditional branch bank with core banking solutions
(D) A payment app using the Unified Payments Interface only

Oct/Nov 2009

**8.** How is electronic commerce affecting the composition of the workforce?
(A) By replacing human workers with intelligent

Downloaded from www.pdf.tube

digital agents
(B) By shifting routine information tasks to complex activities
(C) By ensuring employees spend rigid hours at a physical desk
(D) By increasing manual rote activities in traditional banks

May/June 2017

**9.** Which statement correctly identifies the impact of E-commerce?
(A) It enforces geographical barriers to protect local markets.
(B) It allows customers to overcome geographical barriers and purchase products anytime and from anywhere.
(C) E-commerce markets are growing at a slower rate than traditional markets.
(D) The basic applicability of e-commerce in India is governed by the Banking Regulation Act.

Oct/Nov 2024

**10.** In the world of the internet, what percentage do Deep and dark webs contribute to?
(A) 4%
(B) 88%
(C) 96%
(D) 92%

May/June 2012

**11.** Which statement best illustrates "Choice and convenience" for Web consumers?
(A) An Internet bookstore may carry around 2.5 million titles compared to 150,000 in a chain bookstore.
(B) Consumers must visit a physical branch to balance their accounts daily.
(C) Transferring funds at home incurs heavy transactional fees.
(D) Web consumers are restricted to purchasing out-of-print books exclusively.

Oct/Nov 2019

**12.** What is the Unified Payments Interface (UPI)?
(A) An enterprise data warehouse solution for inter-bank reconciliations
(B) A traditional clearing mechanism for physical cheques
(C) A real-time system by NPCI for inter-bank P2P and P2M transactions
(D) A social networking platform for banking professionals

May/June 2007

**13.** What is a key advantage of "Complete information" for Web consumers?
(A) Comparison of bank rates and services from home in privacy
(B) Direct negotiation with bank staff under perceived pressure
(C) Viewing only out-of-print book titles via restricted lists
(D) Relying on paper catalogues to find competitive market bids

Oct/Nov 2015

**14.** What is the primary purpose of Enterprise-wide Fraud Risk Management (EFRM) solutions in banks?
(A) To eliminate middle managers in the reporting hierarchy
(B) To manage the credit portfolio for higher profitability
(C) To monitor accounts and digital transactions for frauds
(D) To regulate cryptocurrency transactions on a global scale

NODIA

May/June 2020

**15.** Which statement about the computer and video game industry is true?
(A) It remains a highly focused niche market with no impact on the mainstream economy.
(B) It is expected to grow at a Compound Annual Growth Rate of 92% to 2026.
(C) Casual gaming on smartphones has declined significantly in recent years.
(D) Its market size is valued at about USD 174 billion and impacts the economy through hardware and game sales.

Oct/Nov 2005

**16.** What is Mobile Banking?
(A) Remote financial transactions conducted via mobile devices
(B) Service limited to downloading electronic account records
(C) Banking service delivered via physical mobile bank vans
(D) Financial inclusion provided through smart card systems

May/June 2009

**17.** Which statement about the globalization of electronic banking is correct?
(A) It makes it easy for people to keep their money in different countries and currencies.
(B) It restricts individuals to keeping their money in a single currency.
(C) It has completely eradicated cyber hacking and money-heists.
(D) It prevents cross-border shopping and international trade.

Oct/Nov 2012

**18.** How many real-time digital payments did India handle per day in the financial year 2020-2021?
(A) 122 million
(B) 53 million
(C) 86 million
(D) 150 million

May/June 2018

**19.** What is a primary characteristic of workforce globalization in the digital economy?
(A) Physical proximity remains the key to modern convenience
(B) Tasks must be completed by workers in the same country
(C) Banks are prohibited from using support staff in other areas
(D) Borderless internet allows tasks to be completed worldwide

Oct/Nov 2023

**20.** What is the fundamental rationale behind implementing an on-device wallet for UPI?
(A) Decentralizing infrastructure for low-value transaction processing
(B) Increasing the frequency of high-value cross-border transactions
(C) Replacing all banking apps with a single digital currency system
(D) Allowing users to trade stocks directly on international exchanges

May/June 2011

**21.** Which statement regarding the costs of internet banking is correct?
(A) Banking transactions cost more using the Internet than if handled by a teller.
(B) Electronic bill payment increases the biller's printing and mailing costs.
(C) Internet banking reduces administrative costs and paperwork needed for bank transactions.
(D) A website limits a bank's ability to serve thousands of customers each day.

Oct/Nov 2016

**22.** At what rate are e-commerce markets growing compared to traditional markets?
(A) 12.3% against 4%
(B) 21.5% against 2%
(C) 9% against 4%
(D) 55% against 23%

May/June 2025

**23.** How is Information Technology expected to flatten cities?
(A) By replacing all skyscrapers with underground complexes
(B) By increasing real estate prices across all urban areas
(C) By restricting building height using physical sensors
(D) By reducing the need for physical proximity in business

Oct/Nov 2018

**24.** Which statement accurately reflects cyber technology's impact on organizational hierarchy?
(A) It increases the number of middle managers needed for supervision.
(B) It prevents entry-level employees from communicating with the CEO.
(C) It may reduce hierarchy by offering new channels of communication between workers.
(D) It strictly limits communication to formal paper reporting.

May/June 2015

**25.** In the context of workforce flexibility, what have many companies discovered?
(A) That strict office attendance is necessary for high morale
(B) That flexible workplace guidelines best meet customer needs
(C) That telecommuting inevitably decreases employee productivity
(D) That virtual offices increase office space needs and costs

Oct/Nov 2020

**26.** What does Internet banking deliver directly to customers' homes?

Click Here to Buy book on Amazon

(A) Specialized hardware components for networking
(B) Hardcopies of bank statements on a 24-hour basis
(C) Physical smart cards and paper-based checkbooks
(D) Banking services via open-access computer networks

**May/June 2013**

**27.** Which statement correctly describes government control over cyberspace?
(A) Governments have absolute and comprehensive control over all cyberspace activities.
(B) Governments will have only limited control, and tight censorship may be impossible.
(C) Tight censorship on the internet is easily achievable by totalitarians.
(D) Google search indexing covers 4% of the internet, making tracking trivial.

**Oct/Nov 2011**

**28.** How many WhatsApp users are there approximately in India?
(A) 53 crores
(B) 21 crores
(C) 41 crores
(D) 45 crores

**May/June 2006**

**29.** Which statement regarding the Internet of Things (IoT) is correct?
(A) IoT is limited to laptops, smartphones, and tablets.
(B) The number of active IoT endpoints is expected to decline by 2025.
(C) IoT connectivity is strictly confined to fitness trackers.
(D) One of the most important challenges associated with IoT is security.

**Oct/Nov 2007**

**30.** How does the Internet enable one-to-one marketing in retail banking?
(A) By broadcasting uniform promotional materials to all existing customers
(B) By using traditional face-to-face teller interactions for all users
(C) By restricting online product offerings to standardized generic sets
(D) By tracking customer profile data and financial interests to cross-sell

**May/June 2024**

**31.** Which statement regarding AI chatbots in banking is incorrect?
(A) SBI Intelligent Assistant (SIA) helps customers with everyday banking tasks.
(B) HDFC Bank's AI-enabled smart chatbot is called 'Eva'.
(C) 'Eva' works with Google Assistant on millions of Android devices.
(D) Chatbot facilities at banks are strictly available only during banking hours.

**Oct/Nov 2010**

**32.** The Work from Home (WFH) model presents various challenges, EXCEPT:
(A) Managing projects across multiple locations
(B) Securing the connection between the employee and the internal network
(C) Increased motivation and reduced need for office space
(D) Difficult communication and tracking of individual tasks

**May/June 2019**

**33.** Which statement about the *99# short code is incorrect?
(A) It offers mobile banking services on the National Unified USSD Platform (NUUP).
(B) It allows access to banking services with a single number across all banks.
(C) It is limited to functioning only on high-end WAP-supported smartphones.
(D) It works irrespective of the telecom service provider or the region.

**Oct/Nov 2022**

**34.** Which of the following best describes the benefit of "Customization" sought by Web consumers?
(A) Choosing exact service combinations online
(B) Ordering identical products as offline consumers
(C) Paying higher rates per trade to support brokers
(D) Ensuring all communications remain paper-based

**May/June 2008**

**35.** Cyber technologies and IT will impact the business and economy in all the following ways EXCEPT:
(A) Permitting increasing automation of

Downloaded from www.pdf.tube

production via robotic mining and farming machines
(B) Completely eliminating the gap between the rich and the poor globally
(C) Reducing marketing costs and increasing consumer satisfaction
(D) Allowing entry-level employees to communicate directly with the CEO

**Oct/Nov 2017**

**36.** Which scenario best exemplifies the "Choice and convenience" benefit of e-commerce?
(A) Waiting in line at a branch to transfer funds securely
(B) Being unaware of competitive bids due to limited online catalogues
(C) Relying solely on monthly printed statements for account balancing
(D) Accessing millions of online book titles versus limited physical stock

**May/June 2010**

**37.** Which of the following statements is incorrect regarding the future of living standards?
(A) The average person will become increasingly rich due to increased productivity.
(B) People might decide to work less, such as working only 10 hours a week.
(C) There are potential obstacles to an ever-rising living standard.
(D) As the number of drones and wastrels grows, production would rise and living standards accelerate.

**Oct/Nov 2006**

**38.** Internet banking provides customers with all the following benefits EXCEPT:
(A) Less waiting time due to reduced time and place limitations
(B) The ability to physically deposit cash directly into a PC drive
(C) Ease and convenience of transactions from the comfort of home or office
(D) A self-service channel with 24 x 7 availability

**May/June 2016**

**39.** What is the most profound potential impact of applying ICT to government processes (e-Governance)?
(A) Increasing the cost of voting from home
(B) Enhancing government efficiency and accountability
(C) Limiting access to candidate biographies
(D) Tracking individuals for censorship alone

**Oct/Nov 2013**

**40.** Which of the following statements about mobile banking regulations is incorrect?
(A) All bank transactions involving accessing credit/debit through a mobile device are considered mobile-banking transactions.
(B) Licensed banks with Core Banking Solutions (CBS) are permitted to offer mobile-banking services.
(C) Cross-border mobile transfers are currently freely allowed by the RBI.
(D) Banks must obtain permissions from the Department of Payments and Settlement Systems, RBI.

**May/June 2022**

**41.** Arrange the following events in the correct chronological order of their occurrence:
1. IT Act enacted by the Government of India
2. Launch of EASE 4.0
3. Demonetization initiative by GoI
4. Introduction of UPI by NPCI

(A) 1, 3, 4, 2
(B) 1, 4, 3, 2
(C) 3, 1, 4, 2
(D) 4, 3, 1, 2

**Oct/Nov 2025**

**42.** Which statement regarding UPI's internationalization is incorrect?
(A) Only rupee-based services within India are allowed under NIPL's new global framework.
(B) NIPL signed an MoU with PPRO Financial to expand UPI into China and the United States.
(C) Liquid Group signed an MoU to introduce a UPI-based QR code system in multiple Asian countries.
(D) An MoU covering the UAE and other middle east countries will be effective from Q1-2022.

**Oct/Nov 2009**

**43.** Interactive technologies currently adopted by banks include all of the following EXCEPT:
(A) Virtual reality systems that replace all staff
(B) Pin-less ATMs utilizing Biometrics
(C) AI-powered assistants like SIA and Eva

NODIA

(D) Account Opening Kiosks (AOK)

**May/June 2023**

**44.** The impact of IT on money includes all of the following EXCEPT:
(A) Handing much of the financial business automatically via computers
(B) Using smart cards with photographs or fingerprints for purchases and data storage
(C) Replacing all fiat currencies exclusively with video game credits
(D) Computer programs amassing billions on mutual fund trading floors

**Oct/Nov 2018**

**45.** What is the primary reason the RBI issued a directive for UPI mobile apps to support an on-device wallet feature?
(A) To increase the frequency of high-value transactions
(B) To manage complex international currency exchanges
(C) To decentralize back-end low-value UPI processing
(D) To eliminate the use of smartphones for bank tasks

**May/June 2007**

**46.** Which of the following statements about cash transactions in India is incorrect?
(A) Prior to the digital push, cash accounted for upwards of 95% of all transactions.
(B) India handles 122 million cash transactions per day, making it the global leader in cash reliance.
(C) As of date, the percentage of cash transactions still lies around 88%.
(D) Around 85% of workers were paid in cash before the campaign.

**Oct/Nov 2014**

**47.** What constitutes the greatest technological challenge for organizations implementing a Work from Home (WFH) policy?
(A) Providing employees with larger office spaces
(B) Mandating virtual commutes during heavy traffic
(C) Eliminating the need for higher cognitive logic
(D) Securing internal network connections for data

**May/June 2019**

**48.** Which statement about the challenges of Work from Home (WFH) is incorrect?
(A) WFH eliminates the threat of data leakage and attack by adversaries on internal systems.
(B) Keeping track of individual tasks is problematic for complex projects and large teams.
(C) Communication is more difficult without a physical presence.
(D) Securing the connection between the employee and the internal network poses cyber risks.

**Oct/Nov 2006**

**49.** The GoI's EASE reform components underlying 'SMART' banking include all of the following EXCEPT:
(A) Synchronized
(B) Speedy
(C) Multi-channel
(D) Accessible & affordable

**May/June 2021**

**50.** Strategic drivers pushing financial services institutions toward IT change include all of the following EXCEPT:
(A) Increased competition from non-traditional competitors
(B) Changing consumer behaviour demanding round-the-clock service
(C) Reverting from a sales culture to a service culture
(D) Growing pressure from shareholders for improved financial performance

**Oct/Nov 2010**

**51.** What is the most significant impact of Biometrics like the Aadhaar card on the Indian banking sector?
(A) Enabling e-KYC for the Financial Inclusion drive
(B) It eliminates the need for any electronic transactions
(C) It allows for physical tracking of stolen goods globally
(D) It prevents the use of AI chatbots for everyday banking tasks

**May/June 2005**

**52.** Which statement regarding EASE reforms is incorrect?

Click Here to Buy book on Amazon

(A) EASE stands for Enhanced Access and Service Excellence.
(B) The SMART acronym includes Artificial and Monitored services.
(C) CLEAN is meant for credit portfolio management.
(D) The latest version 4.0 of EASE was released during August 2021.

**Oct/Nov 2022**

**53.** Information Technology is expected to have all the following general impacts EXCEPT:
(A) Flattening cities by reducing office needs
(B) Enhancing home comfort and digital security
(C) Adapting automobiles for work and recreation
(D) Requiring physical crowding in urban centers

**May/June 2018**

**54.** What is the main reason online retail banking achieves lower operating costs?
(A) It relies heavily on middle managers for supervision and reporting
(B) Banks increase the usage of physical paper checks for all vendor payments
(C) Online transactions cost significantly less than branch teller services
(D) It requires maintaining large legacy mainframe systems

**Oct/Nov 2016**

**55.** Benefits of Internet banking for banks include all of the following EXCEPT:
(A) Increased profitability and better operating efficiency ratios
(B) A cost-effective mechanism reducing administrative costs and paperwork
(C) Reaching customers where there is no physical branch
(D) Higher transaction costs per customer compared to a branch teller

**May/June 2014**

**56.** Which statement regarding the IT Vision Document 2011-17 is incorrect?
(A) It provides an indicative road map to enhance the usage of IT in the banking sector.
(B) It was prepared by the Dr. K.C. Chakrabarty Committee.
(C) The committee included members from IIM, IDRBT, IIT, and the Reserve Bank.
(D) It mandated the immediate eradication of all traditional banking branches.

NODIA

**Oct/Nov 2007**

**57.** What is cited as the core business justification for industry and operational consolidation in banking and insurance?
(A) Achieving scale through technical consolidation
(B) Increasing excess capacity in the market
(C) Reducing the number of web consumers
(D) Expanding footprints of legacy mainframe servers

**May/June 2025**

**58.** Which of the following statements about interactive technologies for banks is incorrect?
(A) Account Opening Kiosks (AOK) require a minimum of 24 hours to open a savings bank account.
(B) A web-enabled ATM can allow a user to check e-mail and buy a concert ticket.
(C) Pin-less ATMs identify users by reading the iris, finger-print, or retina.
(D) The technology of identifying users by their biological features is called Biometrics.

**Oct/Nov 2019**

**59.** What is the primary reason IT will flatten cities and cut skyscrapers down to size?
(A) Real estate prices have made skyscrapers economically unviable to build
(B) Infrared cameras and microprocessors prohibit high-altitude construction
(C) Digital assistants are unable to process data above a certain physical elevation
(D) Work-from-Home reduces the need for physical business proximity

**May/June 2009**

**60.** IT's impact on government encompasses all of the following EXCEPT:
(A) Providing abundant official information easily to citizens
(B) Allowing far more citizen input via electronic polling and voting
(C) Leveraging digital government for citizen-centric and transparent services
(D) Keeping the society fully closed from external messaging

Oct/Nov 2011

**61.** Match the banking driver/benefit in List-I with its accurate categorization in List-II.
List I: (Driver/Benefit)
P. Reach where there is no branch
Q. One-to-one marketing
R. 24 x 7 Availability
S. Save time and money
List II: (Categorization)
1. Bank benefit (Branchless)
2. Retail online banking driver
3. Customer benefit (Always open)
4. Customer benefit (No traffic)
(A) P-2, Q-3, R-1, S-4
(B) P-1, Q-2, R-3, S-4
(C) P-3, Q-1, R-4, S-2
(D) P-4, Q-2, R-3, S-1

May/June 2010

**62.** Consider the following statements:
I A Neo-bank operates exclusively online without traditional physical branch networks.
II Online banking focuses on digitizing every program and activity, while digital banking digitizes only the "core" aspects of banking.
Which of the statements is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

Oct/Nov 2024

**63.** Match the AI Chatbot or feature in List-I with its associated entity or function in List-II.
List I: (Chatbot/Feature)
P. SIA
Q. Eva
R. AOK
S. NUUP
List II: (Associated Entity/Function)
1. SBI
2. HDFC Bank
3. Account opening in 15 minutes
4. *99#
(A) P-1, Q-2, R-3, S-4
(B) P-2, Q-1, R-4, S-3
(C) P-3, Q-4, R-1, S-2
(D) P-4, Q-3, R-2, S-1

May/June 2017

**64.** Consider the following statements regarding Web consumer benefits:
I Consumers can compare rates and services of different banks at home in one sitting.
II Consumers avoid the perceived pressure of dealing one-on-one with a bank representative.
III Consumers who buy and sell stocks through the Internet commonly pay more per trade than traditional brokerages.
Which of the above statement(s) is/are correct?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) All (I), (II), and (III)

Oct/Nov 2005

**65.** Identify the correct pair of AI Chatbot and its respective bank.
(A) SIA - State Bank of India
(B) SIA - HDFC Bank
(C) Eva - State Bank of India
(D) Eva - ICICI Bank

May/June 2020

**66.** Consider the following statements regarding the EASE reforms:
I EASE stands for Enhanced Access and Service Excellence.
II The CLEAN initiative is meant for credit portfolio management.
III The 'T' in SMART stands for Technology enhanced services to customers.
IV EASE version 4.0 was released during August 2021.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (IV)
(B) (I), (III), and (IV)
(C) (II), (III), and (IV)
(D) All (I), (II), (III), and (IV)

Oct/Nov 2015

**67.** Arrange the following developments in the correct chronological order:
1. IT Vision Document (2011-17) prepared
2. RBI directive for on-device wallet for UPI
3. Demonetization initiative
4. Release of EASE 4.0
(A) 1, 3, 4, 2
(B) 1, 3, 2, 4
(C) 3, 1, 4, 2

Downloaded from www.pdf.tube

(D) 1, 4, 3, 2

May/June 2013

**68.** Consider the following statements:
I Smart houses will automatically sprinkle gardens and adjust heating systems constantly to keep comfortable at the lowest possible cost.
II Self-driven cars will feature infrared cameras to alert the driver if he is dozing off or not paying attention.
Which of the statements is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

Oct/Nov 2021

**69.** Consider the following statements regarding the Internet of Things (IoT):
I IoT connectivity has become the norm and is termed by some as bigger than the industrial revolution.
II The global number of connected IoT devices is expected to grow to 27 billion by 2025.
III One of the most important challenges associated with IoT is security.
Which of the above statement(s) is/are correct?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) All (I), (II), and (III)

May/June 2024

**70.** Match the letter of the SMART acronym in List-I with its meaning in List-II.
List I: (Letter)
P. S
Q. M
R. A
S. R
List II: (Meaning)
1. Speedy
2. Multi-channel
3. Accessible & affordable
4. Responsive
(A) P-1, Q-2, R-3, S-4
(B) P-2, Q-1, R-4, S-3
(C) P-3, Q-4, R-1, S-2
(D) P-4, Q-3, R-2, S-1

NODIA

Oct/Nov 2008

**71.** Consider the following statements regarding Media and Entertainment:
I Ultra-realistic simulations will allow people to spend their lives in fictitious worlds.
II The video game industry market size is valued at about USD 174 billion.
III Casual gaming sees 92% of smartphone owners play games at least once a week.
IV New technologies will allow fans to alter films and recreate voices of dead stars.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (III)
(B) (I), (III), and (IV)
(C) (II), (III), and (IV)
(D) All (I), (II), (III), and (IV)

May/June 2006

**72.** Match the IT phenomenon in List-I with the domain it primarily impacts in List-II.
List I: (Phenomenon)
P. Flattening cities
Q. Intelligent agents sorting catalogues
R. Amassing billions by speed chess algorithms
S. Availability of political candidate biographies
List II: (Impact Domain)
1. General Impact
2. Business and Economy
3. Money
4. Government
(A) P-1, Q-2, R-3, S-4
(B) P-2, Q-1, R-4, S-3
(C) P-3, Q-4, R-1, S-2
(D) P-4, Q-3, R-2, S-1

Oct/Nov 2017

**73.** Consider the following statements:
I Electronic systems will eventually allow voters to vote electronically in their homes, keeping government closer to the people.
II The delivery of a citizen-centric and transparent government is only possible through the extensive use of technology and digital government.
Which of the statements is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

May/June 2008

**74.** Identify the correct pair of social media platform and its approximate user base in India.
(A) Twitter - 2 crores
(B) Instagram - 45 crores
(C) Facebook - 53 crores
(D) YouTube - 21 crores

Oct/Nov 2013

**75.** Consider the following statements regarding the *99# service:
I It stands for the National Unified USSD Platform (NUUP).
II It provides mobile banking services.
III It allows banking customers to access services irrespective of the telecom service provider.
IV It is strictly restricted to smartphone users only.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (IV)
(B) (II), (III), and (IV)
(C) (I), (II), and (III)
(D) (I), (III), and (IV)

May/June 2015

**76.** Match the Social Media platforms in List-I with their approximate user base in India (in crores) in List-II.
List I: (Social Media Platform)
P. WhatsApp
Q. YouTube
R. Facebook
S. Instagram
List II: (User base in crores)
1. 53
2. 45
3. 41
4. 21
(A) P-2, Q-3, R-1, S-4
(B) P-1, Q-2, R-3, S-4
(C) P-3, Q-1, R-4, S-2
(D) P-4, Q-2, R-3, S-1

Oct/Nov 2012

**77.** Consider the following statements regarding workforce flexibility:
I In the digital age, an employee's workday must strictly remain between 8 a.m. and 5 p.m. at a desk.
II Letting go of rigid guidelines traditionally followed in the workplace is the best approach to meeting customer needs.
III Telecommuting programs report an increase in productivity and faster completion of assignments.
Which of the above statement(s) is/are correct?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) All (I), (II), and (III)

May/June 2011

**78.** Match the data point in List-I with its corresponding topic in List-II.
List I: (Data Point)
P. 21.5%
Q. 9%
R. 88%
S. 50%
List II: (Topic)
1. E-commerce market growth rate
2. Global video game market CAGR to 2026
3. Cash transactions percentage as of date
4. Proportion of UPI transactions below Rs. 200
(A) P-1, Q-2, R-3, S-4
(B) P-2, Q-1, R-4, S-3
(C) P-3, Q-4, R-1, S-2
(D) P-4, Q-3, R-2, S-1

Oct/Nov 2020

**79.** Consider the following statements:
I WFH brings benefits such as less commuting time, better work-life balance, and reduced need for office space.
II The biggest challenge with WFH is managing projects when the team is spread out and communication is more difficult.
Which of the statements is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

May/June 2022

**80.** Identify the incorrect pair regarding technology and its characteristic.
(A) IoT - Connected devices like fitness trackers and fridges
(B) Biometrics - Pin-less ATM using iris or fingerprint
(C) EFRM - Enterprise-wide Fraud Risk Management

Click Here to Buy book on Amazon

(D) Deep Web - Accounts for only 4% of the internet

Oct/Nov 2023

**81.** Consider the following statements regarding Cybersecurity and EFRM:

I Criminals are moving into cyberspace to cover tracks using complex international transactions.

II Computer programs survey bank accounts for sudden activity in long-dormant accounts.

III EFRM solutions monitor card and digital transactions for possible frauds.

IV WFH connectivity poses zero risk of data leakage or attack on internal systems.

Which of the above statement(s) is/are correct?

(A) (I), (II), and (III)
(B) (I), (II), and (IV)
(C) (II), (III), and (IV)
(D) (I), (III), and (IV)

May/June 2023

**82.** Match the partner/region in List-I with its associated UPI internationalization detail in List-II.

List I: (Partner/Region)

P. PPRO Financial
Q. Liquid Group
R. UAE
S. NPCI

List II: (Internationalization Detail)

1. UK based (China/US markets)
2. Singapore and other Asian markets
3. Effective from Q1-2022
4. Manages the BHIM app

(A) P-1, Q-2, R-3, S-4
(B) P-2, Q-1, R-4, S-3
(C) P-3, Q-4, R-1, S-2
(D) P-4, Q-3, R-2, S-1

Oct/Nov 2018

**83.** Match the Web consumer benefit in List-I with its corresponding description in List-II.

List I: (Web Consumer Benefit)

P. Customization
Q. Complete information
R. Discounts
S. Choice and convenience

List II: (Description)

1. Exact combination of services
2. Avoid perceived pressure of dealing one-on-one
3. Pay less per trade online
4. Access to millions of titles

(A) P-1, Q-2, R-3, S-4
(B) P-2, Q-1, R-4, S-3
(C) P-3, Q-4, R-1, S-2
(D) P-4, Q-3, R-2, S-1

NODIA

May/June 2007

**84.** Consider the following statements on Biometrics and ATMs:

I A pin-less ATM can recognize the customer by reading the iris, fingerprint, or retina.

II Biometrics identifies users by their biological features.

III Aadhaar card uses biometrics and has enabled e-KYC to drive Financial Inclusion.

Which of the above statement(s) is/are correct?

(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) All (I), (II), and (III)

Oct/Nov 2025

**85.** Consider the following statements:

I Up until the demonetization campaign, India was an incredibly cash-centric economy where cash accounted for upwards of 95% of all transactions.

II Today, India handles about 122 million real-time digital payments per day, meaning cash transactions have dropped to below 10%.

Which of the statements is/are correct?

(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

May/June 2012

**86.** Match the acronym in List-I with its expansion in List-II.

List I: (Acronym)

P. EASE
Q. EFRM
R. NIPL
S. IoT

List II: (Expansion)

1. Enhanced Access and Service Excellence
2. Enterprise-wide Fraud Risk Management
3. NPCI International Payments Limited
4. Internet of Things

(A) P-1, Q-2, R-3, S-4

(B) P-2, Q-1, R-4, S-3
(C) P-3, Q-4, R-1, S-2
(D) P-4, Q-3, R-2, S-1

**Oct/Nov 2014**

**87.** Consider the following statements regarding IT's impact on Business and Economy:
I Global productivity will climb rapidly due to increasing automation of production.
II Technology allows businesses to reach new economic markets and reduces marketing costs.
III E-commerce markets are growing at a rate of about 21.5%.
IV Cyber technology heavily increases hierarchy and the number of middle managers needed in organizations.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (III)
(B) (I), (III), and (IV)
(C) (II), (III), and (IV)
(D) (I), (II), and (IV)

**May/June 2019**

**88.** Match the strategic IT response in List-I with its driving factor or feature in List-II.
List I: (IT Response)
P. RDBMS
Q. Operational consolidation
R. Changing consumer behaviour
S. Improved financial performance
List II: (Driving Factor/Feature)
1. CIS and data warehouse
2. Merger of large institutions
3. Demand for round-the-clock service
4. Revenue enhancements
(A) P-2, Q-3, R-1, S-4
(B) P-1, Q-4, R-2, S-3
(C) P-3, Q-1, R-4, S-2
(D) P-1, Q-2, R-3, S-4

**Oct/Nov 2006**

**89.** Consider the following statements regarding the internationalization of UPI:
I Around 777 million Indian consumers shopped cross-border in 2021.
II NIPL signed an MoU with PPRO Financial to expand UPI into China and the US.
III Liquid Group signed an MoU to introduce a UPI-based QR code system exclusively in European countries.
Which of the above statement(s) is/are correct?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) All (I), (II), and (III)

**May/June 2021**

**90.** Identify the incorrect pair of abbreviation and its expansion.
(A) WFH - Work from Home
(B) WAP - Wireless Application Protocol
(C) NUUP - National Unified USSD Platform
(D) NIPL - National Internet Payments Limited

**Oct/Nov 2010**

**91.** The following question consists of two statements – Assertion (A) and Reason (R). Answer the question selecting the appropriate option given below:
Assertion (A): Cyber technology may reduce hierarchy in organizations.
Reason (R): E-mail allows even entry-level employees to communicate directly with the CEO, bypassing middle managers.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2005**

**92.** To shift to a sales culture, Bank XYZ needs to exploit information as a business asset. Which specific system is prioritized at banks to consolidate and organize customer information?
(A) Basic electronic typewriter systems
(B) Closed-loop cash counting machines
(C) RDBMS-based CIS and data warehouses
(D) Analogue ledger repository systems

**Oct/Nov 2022**

**93.** Consider the following statements regarding GoI and RBI initiatives:
I The IT Act 2000 provided legal recognition to electronic transactions.
II RBI monitors legal requirements of e-banking on a continuous basis.
III The IT Vision Document 2011-17 was prepared by the Dr. K.C. Chakrabarty Committee.

NODIA

IV RBI advises banks to strengthen security aspects in internet banking.
V NPCI is prohibited from enhancing the number of mobile banking services.

Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (IV)
(B) (I), (II), (III), and (V)
(C) (II), (III), (IV), and (V)
(D) (I), (III), (IV), and (V)

**May/June 2018**

**94.** The merchant's business grows, and he begins taking orders from customers in Singapore. To accept UPI payments there, which entity signed an MoU to introduce a UPI-based QR code system in Singapore?
(A) PPRO Financial
(B) US Federal Reserve
(C) Liquid Group
(D) European Central Bank

**Oct/Nov 2016**

**95.** The following question consists of two statements – Assertion (A) and Reason (R). Answer the question selecting the appropriate option given below:
Assertion (A): Financial institutions are placing focus on converting from a service to a sales culture.
Reason (R): It costs much less to retain and expand relationships with an existing customer than to acquire new customers.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2014**

**96.** A Public Sector Bank is revamping its services under the latest EASE guidelines to ensure better customer service. Which component of EASE is specifically meant for credit portfolio management?
(A) SMART
(B) CLEAN
(C) AOK
(D) NUUP

**Oct/Nov 2007**

**97.** Consider the following statements regarding Strategic IT Issues in banks:
I Financial institutions are converting from a service to a sales culture.
II Consolidation of technical operations provides economies of scale.
III Consumers demand service convenience around the clock from home or mobile phones.
IV Institutions are migrating to open client/server architecture and downsizing legacy mainframes.
V Aggressive IT strategies correlate with revenue enhancements and improved efficiency.

Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (V)
(B) (II), (III), IV, and (V)
(C) (I), (III), (IV), and (V)
(D) All (I), (II), (III), (IV), and (V)

**May/June 2025**

**98.** Bank XYZ is going through a massive strategic shift due to increased competition and changing consumer behaviour. Management decides to migrate to an open client/server architecture and implement an enterprise data warehouse. Aggressive selling strategies and fee generation focus correlate closely with which of the following?
(A) Network reengineering and innovative IT use
(B) Increasing the physical number of middle managers
(C) Reverting strictly to legacy mainframe systems
(D) Abandoning all digital channels to reduce costs

**Oct/Nov 2019**

**99.** The startup also wishes to cater to users who do not have internet access on their basic mobile phones. Which short code should they integrate for the National Unified USSD Platform (NUUP)?
(A) *123#
(B) *99#
(C) *88#
(D) *100#

Downloaded from www.pdf.tube

May/June 2009

**100.** The following question consists of two statements – Assertion (A) and Reason (R). Answer the question selecting the appropriate option given below:
Assertion (A): Physical currency will become less popular in the future.
Reason (R): Smart cards and other payment channels like mobile apps will be used to pay for many small purchases.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Oct/Nov 2011

**101.** The bank aims to fulfill all elements of the SMART banking acronym. What does the 'T' in SMART stand for?
(A) Technology enhanced services to customers
(B) Total security of financial transactions
(C) Telecommuting via integration protocols
(D) Total quality management in service desk

May/June 2010

**102.** Consider the following statements regarding Interactive Technology for Banks:
I A Web-enabled ATM can allow users to check e-mail and buy tickets.
II Pin-less ATMs use biometric features like iris or fingerprint.
III EASE reforms focus on SMART banking for better customer service.
IV An Account Opening Kiosk (AOK) can open a savings account in 15 minutes.
V AI chatbots like SIA and Eva address customer queries on a 24 x 7 basis.
Which of the above statement(s) is/are correct?
(A) (I), (II), (IV), and (V)
(B) (II), (III), (IV), and (V)
(C) (I), (III), (IV), and (V)
(D) All (I), (II), (III), (IV), and (V)

Oct/Nov 2024

**103.** Despite the benefits of Bank XYZ's WFH policy, they face issues with team coordination. What is cited as the biggest challenge with WFH?
(A) Managing projects across distant team locations
(B) Increasing the overhead for physical office space
(C) Providing higher commuting subsidies to employees
(D) Implementing standard virtual office technologies

NODIA

May/June 2017

**104.** The following question consists of two statements – Assertion (A) and Reason (R). Answer the question selecting the appropriate option given below:
Assertion (A): RBI issued a directive to eliminate the on-device wallet feature from UPI apps.
Reason (R): 50% of UPI transactions are below Rs. 200, which creates a large backlog of volume and affects network stability.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Oct/Nov 2005

**105.** To protect the merchant and its users from potential cyber frauds, the merchant's bank employs an EFRM solution. What does EFRM stand for?
(A) Electronic Fund Routing Mechanism
(B) Enhanced Financial Reporting Matrix
(C) Enterprise-wide Fraud Risk Management
(D) External Fraud Reduction Methodology

May/June 2020

**106.** Consider the following statements regarding Mobile Banking:
I It allows customers to conduct transactions remotely using a mobile device.
II It usually involves a software application provided by the financial institution.
III It operates over the revolutionary Unified Platform Interface (UPI) introduced by NPCI.
IV It is usually available on a 24-hour basis.
V Cross-border transfers via mobile banking are currently fully allowed by RBI.
Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (V)

(B) (I), (II), (III), and (IV)
(C) (II), (III), (IV), and (V)
(D) (I), (II), (IV), and (V)

**Oct/Nov 2015**

**107.** A rural merchant relies heavily on cash but decides to adopt UPI after receiving a QR code from his bank. The rollout of millions of QR codes has led to significant UPI volume. In June 2021, the number of transactions done through mobile apps hit what number?
(A) 3.7 billion
(B) 1.12 billion
(C) 122 million
(D) 150 million

**May/June 2013**

**108.** The following question consists of two statements – Assertion (A) and Reason (R). Answer the question selecting the appropriate option given below:
Assertion (A): Future online bankers will have a diminished ability to predict and fulfill the needs of individual customers.
Reason (R): One-to-one marketing via the Internet allows a bank to keep track of a customer's address, income, and financial interests.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2021**

**109.** A fintech startup plans to launch a new bank targeting Gen-Z. The startup will have no physical branches and will offer all services via a mobile app. How is this bank classified?
(A) A traditional computerized bank
(B) A regional rural bank
(C) An offline cooperative bank
(D) A Neo-bank or digital bank

**May/June 2024**

**110.** The following question consists of two statements – Assertion (A) and Reason (R). Answer the question selecting the appropriate option given below:
Assertion (A): Web consumers are heavily disadvantaged because they lack information compared to offline counterparts.
Reason (R): It is much easier for a consumer to compare the rates and services of different banks at home in one sitting.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2008**

**111.** Under the SMART initiative, the bank deploys an AI chatbot that acts like a human. This is similar to the AI-powered smart chat assistant deployed by the State Bank of India (SBI). What is SBI's assistant called?
(A) Eva
(B) Alexa
(C) Siri
(D) SIA

**May/June 2006**

**112.** The following question consists of two statements – Assertion (A) and Reason (R). Answer the question selecting the appropriate option given below:
Assertion (A): Information Technology will flatten cities by cutting skyscrapers down to size.
Reason (R): The concept of Work-from-Home (WFH) means business people no longer need to be physically close to each other for easy communication.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2017**

**113.** The following question consists of two statements – Assertion (A) and Reason (R). Answer the question selecting the appropriate option given below:
Assertion (A): The computer and video game

Click Here to Buy book on Amazon

industry has a major impact on the economy.
Reason (R): The global video game market size is valued at about USD 174 billion and expected to grow at a CAGR of 9% to 2026.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2008**

**114.** For users accessing the smartphone app, the startup implements biometric authentication. What biological features are explicitly used for pin-less ATM or similar interactive technologies?
(A) Voice pitch and physical typing speed
(B) Iris of eye, finger-print, or retina
(C) Facial symmetry and distinct hair color
(D) Molecular DNA sequencing technologies

**Oct/Nov 2013**

**115.** Bank XYZ introduces a WFH policy for 40% of their staff to provide workforce flexibility. What is considered the best approach to meeting customer needs through such staff?
(A) Enforcing rigid guidelines traditionally followed in the workplace
(B) Forcing employees to strictly work between 8 a.m. and 5 p.m. at a desk
(C) Requiring all support personnel to relocate to the hometown office
(D) Relaxing rigid guidelines for productivity and morale

**May/June 2015**

**116.** Consider the following statements regarding the explosion of UPI transactions:
I UPI platform had 150 million monthly active users in May 2021.
II Plans are to achieve 500 million UPI users by 2025.
III The proportion of UPI transactions grew from 23% in 2018-19 to 55% in 2020-21.
IV The average value per UPI transaction is around Rs. 1,900.
V Mobile app UPI transactions reached 3.7 billion in June 2021.
Which of the above statement(s) is/are correct?
(A) (I), (II), (IV), and (V)
(B) (II), (III), (IV), and (V)
(C) (I), (III), (IV), and (V)
(D) All (I), (II), (III), (IV), and (V)

**Oct/Nov 2012**

**117.** The merchant is amazed by how fast UPI transfers funds. The Unified Payments Interface (UPI) was introduced by NPCI during which time period?
(A) October 2000
(B) April - August 2016
(C) August 2021
(D) February 2017

**May/June 2011**

**118.** The following question consists of two statements – Assertion (A) and Reason (R). Answer the question selecting the appropriate option given below:
Assertion (A): Governments will have total and comprehensive control over cyberspace.
Reason (R): In the world of the internet, Deep and dark webs contribute to about 96% whereas Google can search only the rest 4%.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2020**

**119.** The target users of the fintech startup predominantly make transactions under Rs. 200. What feature, mandated by an RBI directive, will help the startup's mobile app manage server load and network stability?
(A) An on-device wallet feature
(B) Multi-factor authentication tokens
(C) Physical passbooks for small amounts
(D) E-mail transaction receipts only

**May/June 2022**

**120.** The following question consists of two statements – Assertion (A) and Reason (R). Answer the question selecting the appropriate option given below:
Assertion (A): Organizations implementing WFH face significant cybersecurity risks.
Reason (R): The connection between the

employee and the internal network over the internet can be exploited by adversaries, causing data leakage and loss.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2023**

**121.** At what rate are e-commerce markets growing compared to the 2% growth of traditional markets?
(A) 9%
(B) 55%
(C) 88%
(D) 21.5%

**May/June 2023**

**122.** To further improve customer acquisition, the bank utilizes an Account Opening Kiosk (AOK). How fast can a customer open a savings bank account at an AOK?
(A) 5 minutes
(B) 24 hours
(C) 15 minutes
(D) 48 hours

**Oct/Nov 2009**

**123.** As the chain expands its IoT product line, it faces challenges regarding the data these devices transmit. What is highlighted as one of the most important challenges associated with IoT that must be addressed with priority?
(A) Lack of physical components
(B) High electricity consumption of the WFH model
(C) Security
(D) Inability to connect to the dark web

**May/June 2016**

**124.** A retail consumer electronics chain is moving heavily into e-commerce, anticipating massive growth. They start selling smart appliances (IoT). By 2025, the global number of connected IoT devices is expected to exceed what number?
(A) 27 billion
(B) 12.3 billion
(C) 15 billion
(D) 150 million

**Oct/Nov 2025**

**125.** The chain implements a platform where users can order a specifically built computer system. This corresponds directly to which benefit sought by Web consumers?
(A) Complete information
(B) Customization
(C) Discounts
(D) EFRM

www.nodia.in

Downloaded from www.pdf.tube

# ANSWERS

1. (D) 27 billion
The Internet of Things represents a massive network of interconnected devices ranging from appliances to industrial sensors. Projections indicate a rapid expansion in this sector, with the total count of active endpoints expected to reach twenty-seven billion by twenty-twenty-five. This growth reflects the increasing integration of digital connectivity into everyday physical objects and infrastructure across various global industries and households.

2. (C) By automating garden maintenance and visitor screening
Future residential technology aims to integrate automation for enhanced living standards. Smart homes will utilize sensors and automated systems to handle routine tasks such as watering gardens or screening visitors at the door. These innovations provide residents with higher security levels while simultaneously reducing manual effort and optimizing resource consumption within the domestic environment efficiently through advanced interconnected computer systems and sensors.

3. (C) Enhanced Access and Service Excellence
Public sector banking reforms in India are guided by a specific framework designed to modernize operations and improve customer experiences. This initiative focuses on institutionalizing clean and smart banking practices across the industry. The specific terminology used emphasizes the commitment of these financial institutions toward broadening reach and achieving superior standards in service delivery through technology and improved operational processes.

4. (C) It, coupled with the COVID-119 pandemic, contributed to a multi-fold increase in digital transactions.
The digital payment landscape in India underwent a significant transformation due to specific policy shifts and external health crises. These factors accelerated the adoption of electronic transaction methods among the general population. Consequently, there was a substantial surge in the volume and value of digital payments, moving the economy toward a more cashless and transparent financial system with high efficiency.

5. (B) Because retaining existing customers is more cost-effective
Financial institutions are increasingly prioritizing long-term relationships with their current clientele to maximize profitability. Marketing research indicates that the resources required to maintain and expand services for existing users are significantly lower than the expenses associated with acquiring entirely new customers. This shift necessitates leveraging data to cross-sell products and provide personalized banking experiences for every user through digital platforms.

6. (A) Consumer behaviour shows a growing demand for service convenience and availability around the clock.
Modern banking is shaped by evolving user expectations regarding the accessibility and speed of financial services. Customers now expect to manage their accounts and perform transactions at any time without visiting a physical location. This demand for constant availability compels banks to invest in robust digital infrastructure to remain competitive and meet the needs of a technologically savvy global population.

7. (B) An online bank without traditional physical branch networks
A specialized category of financial institutions has emerged that operates exclusively through digital platforms. These entities provide a full suite of banking services without maintaining any brick-and-mortar office locations. By eliminating physical overhead costs, they focus on delivering seamless mobile and web-based user experiences, distinguishing themselves from traditional banks that use digital tools alongside traditional physical branch networks.

NODIA

8. (B) By shifting routine information tasks to complex activities
The integration of electronic commerce into the economy is fundamentally altering professional responsibilities and skill requirements. Automation handles many repetitive and routine information-processing duties that were previously performed manually. As a result, the workforce is transitioning toward more complex activities that require higher cognitive skills, strategic decision-making, and specialized technical knowledge to manage modern digital business operations effectively and efficiently.

9. (B) It allows customers to overcome geographical barriers and purchase products anytime and from anywhere.
Electronic commerce provides consumers with unprecedented flexibility by removing the limitations of distance and time. Individuals can browse global marketplaces and complete purchases at their convenience without needing to visit a physical store. This accessibility has led to higher growth rates in online markets compared to traditional retail sectors, fundamentally changing how goods and services are distributed globally today.

10. (C) 96%
The visible internet that is indexed by common search engines represents only a tiny fraction of the total digital space. A massive portion of the online world exists below the surface, consisting of non-indexed content and hidden networks used for various purposes. Statistical estimates suggest that this unindexed segment accounts for nearly ninety-six percent of the entire internet content available.

11. (A) An Internet bookstore may carry around 2.5 million titles compared to 150,000 in a chain bookstore.
Online retailers offer a significantly broader range of products compared to physical stores limited by shelf space. This allows consumers to access specialized and rare items that are not typically stocked in traditional outlets. The ability to browse millions of options from a single device provides unmatched convenience and ensures that diverse customer needs and preferences are met effectively and quickly.

12. (C) A real-time system by NPCI for inter-bank P2P and P2M transactions
The National Payments Corporation of India developed a sophisticated system to facilitate immediate fund transfers via mobile devices. This technology enables both person-to-person and person-to-merchant transactions on a twenty-four-hour basis. It acts as a unified platform that integrates multiple bank accounts into a single mobile application, significantly simplifying the digital payment experience for millions of users nationwide through real-time processing.

13. (A) Comparison of bank rates and services from home in privacy
Web consumers benefit from the ability to access detailed data regarding financial products without external interference. This transparency allows individuals to evaluate interest rates and service terms in private, avoiding the direct pressure often felt during face-to-face interactions with bank staff. Comprehensive online information empowers users to make well-informed decisions based on objective comparisons of multiple service providers easily.

14. (C) To monitor accounts and digital transactions for frauds
Modern financial institutions deploy advanced software solutions to safeguard against illegal activities in the digital realm. These systems continuously analyze transaction patterns and account behaviors to identify anomalies that may indicate fraudulent actions. By providing real-time monitoring and alerts, these enterprise-wide tools help banks protect customer assets and maintain the integrity of the broader financial system against evolving cyber threats.

15. (D) Its market size is valued at about USD 174 billion and impacts the economy through hardware and game sales.
The digital entertainment sector has evolved into a major economic force with substantial global market valuation. This industry generates significant revenue through the sale of gaming hardware and software applications across various platforms. Its growth influences other sectors, including telecommunications and retail, while engaging a vast demographic of users who participate in casual and professional gaming activities on smartphones and consoles.

Click Here to Buy book on Amazon

16. (A) Remote financial transactions conducted via mobile devices
Modern technology allows individuals to manage their financial affairs from any location using handheld electronic devices. This service enables users to check balances, transfer funds, and pay bills through dedicated applications or mobile websites. By providing constant access to banking functions without the need for physical visits or desktop computers, it enhances convenience and promotes greater financial inclusion globally.

17. (A) It makes it easy for people to keep their money in different countries and currencies.
The expansion of digital financial services has removed many of the traditional barriers to international trade and personal finance. Individuals can now manage assets across multiple jurisdictions and hold various currencies with relative ease through online platforms. This globalization facilitates seamless cross-border shopping and investment, allowing for more efficient management of personal wealth in an increasingly interconnected world.

18. (A) 122 million
India has emerged as a global leader in the adoption of real-time digital payment systems. High volumes of electronic transactions are processed daily, reflecting a significant shift away from cash-based exchanges. During a specific recent fiscal period, the daily average for these transactions reached a remarkable level, demonstrating the successful integration of technology into the country's economic and financial infrastructure.

19. (D) Borderless internet allows tasks to be completed worldwide
Digital connectivity has revolutionized the way work is organized and executed across the globe. The internet removes physical constraints, enabling companies to utilize talent and resources from different countries simultaneously. This borderless environment allows for continuous operations as tasks are passed between different time zones, resulting in increased efficiency and the ability to serve global markets more effectively.

20. (A) Decentralizing infrastructure for low-value transaction processing
To improve the efficiency of payment networks, financial authorities have introduced features that handle small transactions locally on a user's device. This approach reduces the burden on central banking servers and prevents network congestion during peak times. By managing low-value payments through an on-device mechanism, the system ensures higher success rates and faster processing for everyday financial activities.

21. (C) Internet banking reduces administrative costs and paperwork needed for bank transactions.
Shifting financial activities to digital channels provides significant economic benefits for both banks and their customers. Electronic transactions eliminate the need for physical documentation and manual processing by staff, leading to lower overhead expenses. This streamlined approach allows institutions to operate more efficiently while offering users a cost-effective way to manage their money without the delays of traditional paperwork.

22. (B) 21.5% against 2%
The digital marketplace is expanding at a much faster rate than conventional brick-and-mortar retail sectors. While traditional markets show modest annual growth, e-commerce platforms are experiencing double-digit increases in sales volume and user adoption. This significant disparity highlights the changing consumer preference for the convenience, variety, and competitive pricing offered by online shopping environments compared to physical stores.

23. (D) By reducing the need for physical proximity in business
Information technology is fundamentally changing urban development patterns by enabling remote collaboration. As communication tools become more sophisticated, the necessity for businesses to cluster in expensive city centers decreases. This trend allows for a more distributed workforce and may eventually lead to a reduction in the demand for large office towers, effectively changing the traditional landscape of cities.

Downloaded from www.pdf.tube

**24.** (C) It may reduce hierarchy by offering new channels of communication between workers.
Digital communication tools like electronic mail have significantly altered the structural dynamics within modern organizations. By providing direct channels that bypass traditional layers of management, these technologies allow junior staff to interact with senior executives. This shift contributes to a flatter organizational hierarchy, facilitating faster information flow and more inclusive internal dialogue regardless of an employee's professional rank or position.

**25.** (B) That flexible workplace guidelines best meet customer needs
Many modern enterprises have found that traditional, rigid office requirements are no longer necessary for successful operations. Adopting flexible work arrangements allows employees to be more productive while balancing personal responsibilities. This adaptability often results in better service delivery, as staff can respond to customer demands outside of standard hours, ultimately improving organizational efficiency and employee morale in the digital age.

**26.** (D) Banking services via open-access computer networks
The internet serves as a powerful delivery mechanism for financial products, bringing comprehensive banking capabilities directly to the user. Through secure websites and applications, customers can access a full range of services that were previously only available at physical branches. This model utilizes public and private networks to ensure that financial management tools are accessible from any connected computer.

**27.** (B) Governments will have only limited control, and tight censorship may be impossible.
The decentralized and vast nature of the internet presents significant challenges for state regulatory efforts. While authorities can implement some restrictions, the sheer volume of data and the existence of hidden networks make absolute control extremely difficult to achieve. This environment often limits the effectiveness of tight censorship, as information continues to flow through various alternative channels across global digital borders.

**28.** (A) 53 crores
Messaging applications have seen extraordinary adoption rates in the Indian market, becoming a primary tool for communication. A specific popular platform has reached a massive user base of over five hundred million individuals. This widespread usage reflects the deep penetration of smartphones and mobile data services, which have transformed how citizens interact, conduct business, and share information across the country.

**29.** (D) One of the most important challenges associated with IoT is security.
As the number of connected devices grows, protecting the vast amounts of data they transmit becomes a critical priority. The integration of technology into everyday objects creates new vulnerabilities that can be exploited by malicious actors. Ensuring robust cybersecurity measures for the Internet of Things is essential to prevent data breaches and maintain the privacy and safety of users globally.

**30.** (D) By tracking customer profile data and financial interests to cross-sell
Digital platforms allow banks to gather detailed insights into the habits and needs of their clients. By analyzing this information, financial institutions can create highly personalized marketing strategies that target individuals with specific products. This one-to-one approach increases the effectiveness of sales efforts, as customers receive offers that are relevant to their unique financial goals and interests.

**31.** (D) Chatbot facilities at banks are strictly available only during banking hours.
Artificial intelligence has enabled financial institutions to provide constant support through automated chat interfaces. These virtual assistants are designed to help users with routine tasks and answer queries at any time of the day or night. Unlike traditional branch services, these digital tools operate continuously, ensuring that customers have access to help and information whenever they need it.

**32.** (C) Increased motivation and reduced need for office space
While remote work offers several advantages for organizations and employees, it also introduces

NODIA

specific operational difficulties. Managers must find new ways to coordinate projects and track individual tasks when team members are physically separated. Additionally, establishing secure connections to internal networks and maintaining clear communication channels without face-to-face interaction remain significant hurdles that companies must address to succeed.

**33.** (C) It is limited to functioning only on high-end WAP-supported smartphones.
Mobile banking services in India are designed to be inclusive, reaching users even without advanced technology. A specific short code system utilizes basic telecommunications protocols to provide financial services on any mobile phone, including simple feature phones. This ensures that banking remains accessible to individuals in remote areas or those without internet connectivity, regardless of their service provider.

**34.** (A) Choosing exact service combinations online
Modern electronic commerce platforms allow users to specify unique configurations for their purchases, such as building a computer with specific hardware components. This capability meets the demand for personalized products that cater to individual preferences and requirements. Such customization is a key advantage of online shopping, providing a level of flexibility that is often difficult to achieve in traditional stores.

**35.** (B) Completely eliminating the gap between the rich and the poor globally
While information technology significantly boosts economic productivity and enhances communication, it does not automatically resolve fundamental societal inequalities. Innovations can automate production, reduce business costs, and improve government transparency, but the disparity between different economic classes remains a complex issue. Technology may create new opportunities, but it does not serve as a sole solution for eradicating global poverty or wealth gaps.

**36.** (D) Accessing millions of online book titles versus limited physical stock
Online retailers offer a significantly broader range of products compared to physical stores limited by shelf space. This allows consumers to access specialized and rare items that are not typically stocked in traditional outlets. The ability to browse millions of options from a single device provides unmatched convenience and ensures that diverse customer needs and preferences are met effectively and quickly.

**37.** (D) As the number of drones and wastrels grows, production would rise and living standards accelerate.
While technological progress generally leads to increased productivity and wealth, several factors can impede continuous improvement in living standards. A society's overall well-being depends on the active participation and contribution of its members to the economy. If a large portion of the population becomes unproductive, it can strain resources and slow down the rate of economic and social advancement.

**38.** (B) The ability to physically deposit cash directly into a PC drive
Digital banking provides numerous benefits such as constant availability and the convenience of performing transactions from any location. Users can transfer funds, pay bills, and view statements electronically without waiting in lines at a branch. However, physical activities like handling actual paper currency still require specialized hardware like automated teller machines or traditional teller visits to be processed.

**39.** (B) Enhancing government efficiency and accountability
The application of information technology to public administration can lead to more transparent and responsive governance. By digitizing services and providing easy access to official data, authorities can improve the speed and accuracy of their operations. This digital approach also allows for greater citizen participation and makes it easier to hold officials accountable for their actions and decisions.

**40.** (C) Cross-border mobile transfers are currently freely allowed by the RBI.
Mobile banking in India is subject to specific regulatory requirements to ensure security and financial stability. Banks must use secure core systems and obtain necessary permissions from central authorities before offering these services. While many domestic transactions are facilitated

Click Here to Buy book on Amazon

through mobile apps, there are strict limitations and controls placed on international fund transfers to prevent illegal financial movements.

**41.** (B) 1, 4, 3, 2
The evolution of digital banking in India followed a specific timeline starting with legal frameworks like the Information Technology Act in two thousand. This was followed by the launch of the Unified Payments Interface in twenty-sixteen to revolutionize mobile payments. Subsequent events included the demonetization initiative and later advancements in public sector reforms like the fourth version of EASE in twenty-twenty-one.

**42.** (A) Only rupee-based services within India are allowed under NIPL's new global framework.
India's unified payment system is expanding its reach beyond domestic borders through strategic partnerships with international financial entities. New frameworks allow for the integration of this technology into foreign markets, facilitating cross-border transactions for travelers and residents alike. These agreements aim to establish a global presence for Indian digital payment solutions, enabling seamless financial exchanges in multiple countries.

**43.** (A) Virtual reality systems that replace all staff
Financial institutions are adopting various interactive technologies to improve service delivery and security. Examples include kiosks that allow for rapid account opening and biometric systems for user identification. While artificial intelligence and automated assistants are increasingly used to handle customer queries, they are designed to complement human staff rather than completely replace the entire workforce with virtual reality systems.

**44.** (C) Replacing all fiat currencies exclusively with video game credits
Technology has profoundly changed how money is managed and moved within the global economy. Computer programs now handle vast amounts of financial trading automatically, and smart cards have replaced cash for many daily purchases. While digital currencies and electronic credits exist in specialized environments, they have not replaced the fundamental national currencies issued by governments for general economic use.

NODIA

**45.** (C) To decentralize back-end low-value UPI processing
To improve the efficiency of payment networks, financial authorities have introduced features that handle small transactions locally on a user's device. This approach reduces the burden on central banking servers and prevents network congestion during peak times. By managing low-value payments through an on-device mechanism, the system ensures higher success rates and faster processing for everyday financial activities for users.

**46.** (B) India handles 122 million cash transactions per day, making it the global leader in cash reliance.
Historically, the Indian economy relied heavily on physical currency for the vast majority of its financial activities. A very large percentage of transactions and wage payments were conducted in cash before the recent digital push. However, with the rapid adoption of electronic payment systems, the country has transitioned toward digital methods, handling a massive number of electronic payments daily.

**47.** (D) Securing internal network connections for data
Transitioning to remote work models requires organizations to prioritize the protection of sensitive information. The primary technological hurdle involves establishing and maintaining secure digital links between employees working from various locations and the company's internal servers. Preventing unauthorized access and data breaches in these distributed environments is critical for maintaining operational integrity and protecting confidential business and customer data.

**48.** (A) WFH eliminates the threat of data leakage and attack by adversaries on internal systems.
Remote work arrangements introduce new vulnerabilities that can be exploited by cyber criminals. When employees access internal systems from outside the traditional office environment, the risk of data leakage and unauthorized intrusion increases. Organizations must implement robust security protocols and monitoring systems to mitigate these threats, as working from home does not inherently protect against sophisticated digital attacks.

**49.** (A) Synchronized
Public sector banking reforms in India use a specific acronym to describe the goals of modern service delivery. This framework emphasizes speed, accessibility, and the use of multiple channels to reach customers. By focusing on these elements, banks aim to provide responsive and affordable services that meet the diverse needs of the population while leveraging advanced technology to improve overall efficiency.

**50.** (C) Reverting from a sales culture to a service culture
Financial institutions are driven to change by several strategic factors, including heightened competition and evolving customer expectations. There is also increasing pressure from shareholders to deliver better financial results. To address these challenges, banks are moving toward proactive sales-oriented models that leverage data to better serve clients, rather than simply maintaining traditional reactive service-based approaches to banking.

**51.** (A) Enabling e-KYC for the Financial Inclusion drive
The integration of biological identification systems has transformed the way people access financial services. By using unique physical features for verification, banks can now confirm identities electronically and instantaneously. This advancement is particularly crucial for reaching individuals in underserved areas, allowing them to open accounts and access banking services without the need for extensive physical documentation or traditional branch visits.

**52.** (B) The SMART acronym includes Artificial and Monitored services.
Reforms in the banking sector are structured around specific principles designed to enhance service quality and operational effectiveness. These initiatives include frameworks for clean credit management and the adoption of smart technologies to serve customers better. The latest versions of these guidelines continue to evolve, incorporating new digital strategies to ensure that financial institutions remain responsive to the needs of modern society.

**53.** (D) Requiring physical crowding in urban centers
Information technology is expected to provide greater flexibility in where and how people live and work. By reducing the need for constant physical proximity in business, it may lead to a decrease in urban density and the demand for traditional office space. Instead, technology will enhance home environments and personal transport, allowing for a more distributed and comfortable lifestyle across different regions.

**54.** (C) Online transactions cost significantly less than branch teller services
Digital banking platforms allow financial institutions to process transactions at a fraction of the cost associated with traditional methods. By automating routine tasks and reducing the need for physical branch infrastructure and staffing, banks can improve their overall efficiency. This shift to electronic channels enables institutions to offer competitive services while maintaining lower operating expenses compared to manual teller-based operations.

**55.** (D) Higher transaction costs per customer compared to a branch teller
Adopting internet banking provides numerous advantages for financial institutions, including the ability to reach customers in remote areas without physical branches. It serves as a cost-effective way to manage transactions while reducing the administrative burden and paperwork. Furthermore, these digital channels typically result in lower costs per transaction compared to those handled manually by tellers at a physical location.

**56.** (D) It mandated the immediate eradication of all traditional banking branches.
Strategic documents in the banking sector have provided roadmaps for enhancing the use of information technology. These plans were developed by expert committees to guide institutions toward modernizing their infrastructure and services. While they emphasize the importance of digital adoption and strengthening security, they do not require the immediate removal of all physical branches, which continue to serve specific functions.

Downloaded from www.pdf.tube

**57.** (A) Achieving scale through technical consolidation
Large financial institutions are merging their operations to achieve greater efficiency through shared technology and infrastructure. By consolidating their technical systems, these organizations can handle larger volumes of data and transactions more cost-effectively. This process helps them maintain a competitive edge in the global market by reducing redundant systems and leveraging economies of scale in their IT investments.

**58.** (A) Account Opening Kiosks (AOK) require a minimum of 24 hours to open a savings bank account.
Interactive technologies in banking are designed for speed and convenience. Modern kiosks can facilitate the opening of accounts very quickly, often within fifteen minutes. Additionally, biometric systems use unique biological traits like fingerprints or iris patterns to verify users at automated machines. These advancements allow for a more personalized and secure banking experience that is accessible outside of traditional hours.

**59.** (D) Work-from-Home reduces the need for physical business proximity
The rise of remote work enabled by digital connectivity is changing the demand for traditional commercial real estate. As business communication no longer requires face-to-face interaction in a single location, the necessity for massive office buildings in city centers is declining. This shift allows for a more decentralized workforce and may ultimately lead to a transformation in the architectural landscape of major cities.

**60.** (D) Keeping the society fully closed from external messaging
Digital government initiatives aim to make public services more transparent, efficient, and accessible to the population. By providing official information online and allowing for electronic citizen input, authorities can foster greater engagement and accountability. Technology helps create a more open society where information flows freely, rather than restricting communication or isolating citizens from external messages and global digital interactions.

**61.** (B) P-1, Q-2, R-3, S-4
Modern banking strategies and customer benefits are closely linked through technology. Banks benefit from being able to reach customers without physical branches, while online drivers focus on personalized marketing. For consumers, digital channels provide constant availability and the ability to save time and money by performing transactions from any location without the need to travel to a physical bank office.

**62.** (A) Only (I)
A specialized category of financial institutions has emerged that operates exclusively through digital platforms. These entities provide a full suite of banking services without maintaining any brick-and-mortar office locations. While digital banking involves the comprehensive digitization of all banking programs and activities, these specific branchless banks represent a unique model focused entirely on the online and mobile user experience.

**63.** (A) P-1, Q-2, R-3, S-4
Financial institutions in India have deployed various AI-powered assistants and specialized kiosks to improve customer service. Large public and private banks use these virtual tools to answer queries continuously. Furthermore, automated terminals can process new accounts in a very short time, while specific mobile protocols allow for inclusive banking services that work across different telecom providers using simple short codes.

NODIA

**64.** (A) Only (I) and (II)
Web consumers benefit from the ability to access detailed data regarding financial products without external interference. This transparency allows individuals to evaluate interest rates and service terms in private, avoiding the direct pressure often felt during face-to-face interactions with bank staff. Furthermore, online platforms typically offer lower costs for activities like stock trading compared to traditional full-service brokerage firms.

**65.** (A) SIA - State Bank of India
Artificial intelligence has enabled financial institutions to provide constant support through automated chat interfaces. A specific intelligent assistant was developed by India's largest public

sector bank to help users with their daily banking tasks and queries. These digital tools ensure that help is available at any time, enhancing the overall user experience and improving the efficiency of bank operations.

**66.** (D) All (I), (II), (III), and (IV)
Banking reforms are structured around a comprehensive framework designed to enhance service excellence and operational cleanliness. This includes using technology to provide accessible and responsive services to all customers. The latest iterations of these guidelines, released recently, continue to push for modernization and smarter credit management to ensure that financial institutions remain robust and customer-centric in the digital age.

**67.** (A) 1, 3, 4, 2
The transformation of the financial sector followed a logical progression from initial planning to widespread implementation of digital tools. Early strategic documents laid the groundwork, which was followed by major policy initiatives and the launch of refined service frameworks. The introduction of localized features for payment apps came as a response to the massive volume of small transactions processed by these systems.

**68.** (C) Both (I) and (II)
Future advancements in technology will significantly improve both domestic living and transportation safety. Smart home systems will automatically manage garden maintenance and temperature control to optimize costs and comfort. Similarly, advanced vehicles will utilize internal monitoring systems to detect driver fatigue and ensure attention, thereby enhancing overall safety on the roads through the integration of sophisticated sensors and real-time data processing.

**69.** (D) All (I), (II), and (III)
The Internet of Things is a transformative force that connects a vast number of devices globally. This network is expected to grow to billions of active endpoints by twenty-twenty-five, impacting both industrial and personal environments. However, as this connectivity becomes the norm, addressing the security challenges associated with these devices is essential to protect data and ensure the safe operation of interconnected systems.

**70.** (A) P-1, Q-2, R-3, S-4
Modern service delivery in the banking sector is defined by a set of core principles represented by a specific acronym. These principles focus on ensuring that services are fast, accessible, and delivered through multiple channels. Additionally, the framework emphasizes responsiveness to customer needs, ensuring that financial products are both affordable and efficient for a wide range of users across the country.

**71.** (D) All (I), (II), (III), and (IV)
The digital entertainment industry is experiencing rapid growth and technological evolution. High-value market projections and widespread casual gaming on smartphones highlight its economic importance. Furthermore, advanced simulations and new creative tools are changing how stories are told and how audiences interact with media, allowing for highly personalized experiences and the recreation of voices and environments in ways previously not possible.

**72.** (A) P-1, Q-2, R-3, S-4
Information technology has broad impacts across multiple domains of society. It changes urban landscapes by reducing the need for physical proximity and transforms business by using intelligent tools to manage information. In the financial sector, it enables high-speed automated trading, while in government, it improves transparency by making candidate and policy information easily available to the voting public.

**73.** (C) Both (I) and (II)
Digital government initiatives aim to make public services more transparent, efficient, and accessible to the population. By providing official information online and allowing for electronic citizen input, authorities can foster greater engagement and accountability. Technology helps create a more open society where information flows freely, and eventually, electronic systems may allow for secure voting from the comfort of one's home.

Click Here to Buy book on Amazon

**74.** (A) Twitter - 2 crores
Social media platforms have established a significant presence in India, with user bases numbering in the millions and hundreds of millions. These digital networks are used for a variety of purposes, including communication, entertainment, and the dissemination of information. The specific number of active users on each platform reflects their popularity and the extensive reach of digital connectivity among different demographics.

**75.** (C) (I), (II), and (III)
Mobile banking services in India are designed to be inclusive, reaching users even without advanced technology. A specific platform utilizes basic telecommunications protocols to provide financial services on any mobile phone, including simple feature phones. This ensures that banking remains accessible to individuals regardless of their service provider or region, facilitating greater financial inclusion through a unified and simple-to-use interface.

**76.** (B) P-1, Q-2, R-3, S-4
Messaging and social media applications have seen extraordinary adoption rates in the Indian market. Various platforms for video sharing, social networking, and instant communication have reached massive user bases across the country. These figures demonstrate the deep penetration of mobile data and smartphones, which have fundamentally transformed how citizens interact, share content, and conduct their daily personal and professional activities.

**77.** (B) Only (II) and (III)
Many modern enterprises have found that traditional, rigid office requirements are no longer necessary for successful operations. Adopting flexible work arrangements allows employees to be more productive while balancing personal responsibilities. This adaptability often results in better service delivery and faster completion of assignments, as staff can work in environments that best suit their productivity and meeting diverse customer needs.

**78.** (A) P-1, Q-2, R-3, S-4
Statistical data reveals the rapid growth and changing patterns in the digital economy. While e-commerce and gaming markets show strong annual increases, the traditional reliance on cash transactions is gradually shifting. Furthermore, the high volume of small-value electronic payments highlights the need for efficient processing features in digital wallets to maintain system stability and provide a better user experience.

**79.** (C) Both (I) and (II)
While remote work offers several advantages for organizations and employees, such as reduced commuting and better balance, it also introduces specific operational difficulties. Managers must find new ways to coordinate projects and track tasks when team members are spread out. Effective communication without a physical presence remains a significant hurdle that companies must address to maintain efficiency in a distributed work environment.

**80.** (D) Deep Web - Accounts for only 4% of the internet
The visible internet that is indexed by common search engines represents only a tiny fraction of the total digital space. A massive portion of the online world exists below the surface, consisting of non-indexed content and hidden networks. Statistical estimates suggest that this unindexed segment, known as the deep web, accounts for nearly ninety-six percent of the entire internet content available globally.

**81.** (I), (II), and (III)
Transitioning to remote work models requires organizations to prioritize the protection of sensitive information. Criminals use the complexity of cyberspace to hide their activities, making it necessary for banks to use advanced monitoring systems for digital transactions. However, working from home introduces risks of data leakage that must be managed, as external connections can be exploited by adversaries to attack internal systems.

**82.** (A) P-1, Q-2, R-3, S-4
India's unified payment system is expanding its reach beyond domestic borders through strategic partnerships with international financial entities. New frameworks allow for the integration of this technology into foreign markets across Asia and the Middle East. These agreements aim to establish a global presence for Indian

NODIA

digital payment solutions, enabling seamless financial exchanges for users traveling abroad or conducting international business.

**83.** (A) P-1, Q-2, R-3, S-4
Online platforms offer several key benefits that enhance the consumer experience. Users can customize their purchases to meet specific needs and access a vast amount of information to make better decisions. Furthermore, the digital marketplace provides significant convenience and variety, allowing individuals to browse millions of titles and enjoy discounts that are often not available in traditional physical retail stores.

**84.** (D) All (I), (II), and (III)
The integration of biological identification systems has transformed the way people access financial services and identify themselves at automated machines. By using unique physical features like fingerprints or iris patterns for verification, banks can now confirm identities electronically and instantaneously. This advancement is particularly crucial for driving financial inclusion, as it allows for secure and convenient access to services nationwide.

**85.** (A) Only (I)
Historically, the Indian economy relied heavily on physical currency for the vast majority of its financial activities. A very large percentage of transactions were conducted in cash before the recent digital push. While the adoption of electronic payment systems has grown rapidly, leading to millions of digital payments daily, physical currency still plays a significant role in many parts of the economy today.

**86.** (A) P-1, Q-2, R-3, S-4
Various terms and entities play a critical role in the modernization of the financial and technological landscape. These include frameworks for banking excellence, advanced systems for fraud risk management, and the growth of interconnected devices. Additionally, specialized subsidiaries manage the international expansion of payment systems, ensuring that Indian digital innovations are available to a global audience through strategic partnerships.

NODIA

**87.** (A) (I), (II), and (III)
Technology significantly boosts economic productivity by automating production and allowing businesses to reach new markets more efficiently. The rapid growth of e-commerce markets highlights the changing consumer preference for digital platforms. Furthermore, rather than increasing hierarchy, cyber technologies can lead to flatter organizational structures by providing new communication channels that bypass traditional layers of management and middle-level supervision.

**88.** (D) P-1, Q-2, R-3, S-4
Financial institutions are driven to change by several strategic factors, including heightened competition and evolving customer expectations for constant service. To address these challenges, banks are moving toward proactive sales-oriented models and consolidating their technical operations. These responses are closely linked to the need for better financial performance and the effective use of data through centralized information systems.

**89.** (A) Only (I) and (II)
The expansion of digital payment systems into international markets is driven by the large number of consumers engaging in cross-border shopping. Strategic agreements with foreign financial firms are helping to introduce these payment methods into major global economies. These partnerships aim to provide a seamless transaction experience for users in various countries, although initial rollouts may focus on specific regions or types of services.

**90.** (D) NIPL - National Internet Payments Limited
Various abbreviations are used to describe the technologies and organizations involved in the digital economy. These include models for remote work, communication protocols for mobile devices, and platforms for inclusive banking services. It is important to correctly identify the entities responsible for managing international expansions, as they play a key role in bringing domestic financial innovations to a global audience.

**91.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Digital communication tools like electronic mail have significantly altered the structural dynamics within modern organizations. By providing direct channels that bypass traditional layers of management, these technologies allow junior staff to interact with senior executives. This shift contributes to a flatter organizational hierarchy, facilitating faster information flow and more inclusive internal dialogue regardless of an employee's professional rank or position.

**92.** (C) RDBMS-based CIS and data warehouses
To transition toward a proactive sales culture, financial institutions must effectively manage and analyze large volumes of user information. Advanced database systems and centralized data repositories are essential for organizing this data into a valuable business asset. These tools allow banks to gain insights into customer needs and behaviors, enabling more targeted marketing and better delivery of personalized financial services.

**93.** (A) (I), (II), (III), and (IV)
Government and regulatory bodies in India have taken several steps to support the growth and security of electronic banking. This includes providing legal recognition for digital transactions and offering strategic roadmaps for the use of technology in the sector. These authorities continuously monitor the environment and advise banks on strengthening their security measures to protect users and maintain trust.

**94.** (C) Liquid Group
Strategic partnerships with international financial technology companies are facilitating the global adoption of Indian payment systems. By signing agreements with local providers in various regions, the system can be integrated into existing merchant networks through QR code technologies. This allows travelers and residents to use familiar payment methods when shopping abroad, starting with several countries in the Asian market and beyond.

**95.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Financial institutions are increasingly prioritizing long-term relationships with their current clientele to maximize profitability. Marketing research indicates that the resources required to maintain and expand services for existing users are significantly lower than the expenses associated with acquiring entirely new customers. This shift necessitates leveraging data to cross-sell products and provide personalized banking experiences for every user through digital platforms.

**96.** (B) CLEAN
Reforms in the banking sector include specific initiatives designed to improve the quality of credit portfolios and overall institutional health. By focusing on clean and transparent lending practices, banks can better manage risks and ensure long-term stability. These guidelines work alongside other digital strategies to modernize service delivery and ensure that financial institutions operate with the highest standards of integrity and efficiency.

**97.** (D) All (I), (II), (III), (IV), and (V)
Financial institutions are facing several strategic issues as they adapt to a digital-first world. This includes shifting to sales-oriented cultures, consolidating operations for efficiency, and meeting customer demands for constant service. To succeed, banks are modernizing their technology architecture and adopting aggressive IT strategies that are closely linked to improved financial performance and better revenue generation in a competitive market.

**98.** (A) Network reengineering and innovative IT use
To remain competitive and improve financial results, banks are adopting aggressive strategies that focus on proactive selling and fee generation. These efforts are supported by significant investments in new technology and the redesign of internal networks. By leveraging innovative digital tools, institutions can operate more efficiently and better serve the evolving needs of their customers in a rapidly changing global financial landscape.

Downloaded from www.pdf.tube

**99.** (B) *99#
Mobile banking services in India are designed to be inclusive, reaching users even without advanced technology or internet access. A specific short code system utilizes basic telecommunications protocols to provide financial services on any mobile phone. This ensures that banking remains accessible to individuals in remote areas or those using simple devices, facilitating greater financial participation through a unified interface.

**100.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
The shift toward digital payment methods is reducing the public reliance on traditional physical banknotes and coins. Modern technologies such as smart cards and mobile banking applications provide more convenient ways to handle even minor daily transactions. As these electronic channels become more ubiquitous and user-friendly, the popularity of cash naturally declines in favor of faster, more secure digital alternatives.

**101.** (A) Technology enhanced services to customers
Modern service delivery in the banking sector is defined by a set of core principles that include the use of advanced digital tools to improve the user experience. By enhancing services through technology, banks can provide more responsive, efficient, and accessible financial products. This focus on technological advancement is a key part of the broader effort to modernize public sector banking in India.

**102.** (D) All (I), (II), (III), (IV), and (V)
Financial institutions are adopting various interactive technologies to improve service delivery and security. This includes kiosks for rapid account opening and biometric systems for user identification at automated machines. Furthermore, AI-powered assistants provide continuous support for customer queries. These advancements are part of a broader reform effort to ensure that banking services are smart, responsive, and available on a twenty-four-hour basis.

**103.** (A) Managing projects across distant team locations
While remote work offers several advantages for organizations, it also introduces specific operational difficulties that can impact team coordination. The primary challenge involves managing complex projects when team members are physically separated and communication is more difficult. Organizations must implement effective collaboration tools and management strategies to ensure that tasks are tracked and projects are completed efficiently in a distributed environment.

**104.** (D) Assertion (A) is false, but Reason (R) is true.
To improve the efficiency of payment networks, financial authorities have introduced features that handle small transactions locally on a user's device. A very large proportion of payment transactions are for small amounts, which can create a significant volume of traffic on central servers. By managing these low-value payments through an on-device mechanism, the system ensures higher success rates and better network stability.

**105.** (C) Enterprise-wide Fraud Risk Management
Modern financial institutions deploy advanced software solutions to safeguard against illegal activities in the digital realm. These systems continuously analyze transaction patterns across the entire organization to identify anomalies that may indicate fraudulent actions. By providing real-time monitoring and alerts, these enterprise-wide tools help banks protect customer assets and maintain the integrity of the broader financial system against evolving cyber threats.

**106.** (B) (I), (II), (III), and (IV)
Modern technology allows individuals to manage their financial affairs from any location using handheld electronic devices and dedicated software applications. These services are typically available on a twenty-four-hour basis, providing constant access to various banking functions. However, while domestic transactions are easily facilitated, international transfers are subject to specific regulatory controls to ensure security and prevent illegal financial movements across global borders.

NODIA

**107.** (A) 3.7 billion
The adoption of mobile payment applications has seen extraordinary growth, with transaction volumes reaching massive levels in a very short period. This reflects the successful integration of digital technology into the daily lives of millions of people. High-frequency usage for both personal and merchant payments has transformed the economic landscape, making real-time electronic transactions a standard part of the financial system.

**108.** (D) Assertion (A) is false, but Reason (R) is true.
Digital platforms allow banks to gather detailed insights into the habits and needs of their clients by tracking profile data and financial interests. This information enables financial institutions to create highly personalized marketing strategies that target individuals with specific products. Far from diminishing their ability to fulfill needs, one-to-one marketing via the internet enhances the bank's capacity to provide relevant and timely services.

**109.** (D) A Neo-bank or digital bank
A specialized category of financial institutions has emerged that operates exclusively through digital platforms and mobile applications. These entities provide a full suite of banking services without maintaining any brick-and-mortar office locations. By eliminating physical overhead costs, they focus on delivering seamless and modern user experiences, distinguishing themselves from traditional banks that use digital tools alongside their physical branch networks.

**110.** (D) Assertion (A) is false, but Reason (R) is true.
Web consumers have a significant advantage in accessing detailed information about financial products and services compared to traditional offline customers. Online platforms allow individuals to easily compare interest rates and service terms from multiple providers in a single sitting from their homes. This transparency and ease of access to data empower users to make more informed decisions about their financial choices.

**111.** (D) SIA
Artificial intelligence has enabled financial institutions to provide constant support through automated chat interfaces. A specific intelligent assistant was developed by India's largest public sector bank to help users with their daily banking tasks and queries on a twenty-four-hour basis. These digital tools ensure that help is always available, enhancing the overall user experience and improving the efficiency of bank operations through automation.

**112.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Information technology is fundamentally changing urban development patterns by enabling remote collaboration and work-from-home models. As digital communication tools become more sophisticated, the necessity for business people to be physically close to each other for effective interaction decreases. This trend allows for a more distributed workforce and may eventually lead to a reduction in the demand for traditional office towers.

**113.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
The digital entertainment sector has evolved into a major economic force with a substantial global market valuation and strong growth projections. This industry generates significant revenue through the sale of gaming hardware and software applications across various platforms. Its economic impact is felt through job creation and technological innovation, as it engages a vast and growing demographic of global users.

**114.** (B) Iris of eye, finger-print, or retina
Interactive technologies in the banking sector utilize unique biological features to verify the identity of users at automated machines. By reading physical traits such as fingerprints or patterns in the eye, these systems provide a high level of security without the need for traditional personal identification numbers. This biometric approach ensures that only authorized individuals can access sensitive financial information or perform transactions.

**115.** (D) Relaxing rigid guidelines for productivity and morale
Many modern enterprises have found that traditional, rigid office requirements are no longer necessary for successful operations in

Click Here to Buy book on Amazon

a digital-first environment. Adopting flexible work arrangements and relaxing strict guidelines allows employees to be more productive and enhances their overall morale. This adaptability often leads to better service delivery, as staff can more effectively meet customer needs while maintaining a better work-life balance.

**116.** (D) All (I), (II), (III), and (IV)
The growth of real-time payment systems in India has been extraordinary, with millions of monthly active users and high transaction volumes. Plans to further expand the user base demonstrate the long-term commitment to digital finance. The increasing proportion of these transactions in the overall payment mix, along with significant transaction values, highlights the fundamental shift toward electronic methods for everyday financial activities.

**117.** (B) April - August 2016
The introduction of a unified mobile payment platform in India marked a major milestone in the country's digital journey. Launched several years ago, this system revolutionized how funds are transferred between bank accounts in real-time. Since its initial rollout, it has seen massive adoption by both individual users and merchants, becoming a central part of the nation's modern financial infrastructure and economy.

**118.** (D) Assertion (A) is false, but Reason (R) is true.
The decentralized and vast nature of the internet presents significant challenges for state regulatory efforts and comprehensive control. A massive portion of the online world exists below the surface, consisting of non-indexed content and hidden networks that are not easily tracked by traditional search engines. This environment limits the effectiveness of government censorship, as information continues to flow through various alternative digital channels.

**119.** (A) An on-device wallet feature
To improve the efficiency of payment networks, financial authorities have introduced features that handle small transactions locally on a user's device. This approach reduces the burden on central banking servers and prevents network congestion during peak times. By managing low-value payments through an on-device mechanism, the system ensures higher success rates and faster processing for the large volume of everyday small financial activities.

**120.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Transitioning to remote work models requires organizations to prioritize the protection of sensitive information from external threats. Establishing secure digital links between employees working from home and the company's internal servers is critical, as these connections can be exploited by adversaries. Preventing unauthorized access and potential data leakage is essential for maintaining the operational integrity and security of business and customer data.

**121.** (D) 21.5%
The digital marketplace is expanding at a much faster rate than conventional brick-and-mortar retail sectors. While traditional markets show modest annual growth, e-commerce platforms are experiencing significant double-digit increases in sales volume. This disparity highlights the changing consumer preference for the convenience and variety offered by online shopping environments compared to physical stores, driving a fundamental shift in how global commerce is conducted.

**122.** (C) 15 minutes
Automated kiosks have revolutionized the process of onboarding new customers in the banking sector. These digital terminals utilize interactive technology to verify documents and capture necessary data without manual intervention. By streamlining the verification steps, such systems enable individuals to open a functional savings bank account in a very short time, significantly enhancing efficiency and improving overall customer satisfaction and accessibility.

**123.** (C) Security
As the number of connected devices in the Internet of Things grows, protecting the vast amounts of data they transmit becomes a critical priority. The integration of technology into everyday objects creates new vulnerabilities that can be exploited by malicious actors. Ensuring robust cybersecurity measures is essential to

NODIA

prevent data breaches and maintain the privacy and safety of users in an interconnected world.

**124.** (A) 27 billion
The Internet of Things represents a massive network of interconnected devices ranging from personal appliances to complex industrial sensors. Projections indicate a rapid expansion in this sector, with the total count of active endpoints expected to reach twenty-seven billion by twenty-twenty-five. This growth reflects the increasing integration of digital connectivity into everyday physical objects and infrastructure across global industries and households.

**125.** (B) Customization
Modern electronic commerce platforms allow users to specify unique configurations for their purchases, such as building a computer with specific hardware components. This capability meets the demand for personalized products that cater to individual preferences and requirements. Such flexibility is a key advantage of online shopping, providing a level of personalization that is often difficult to achieve through traditional, standardized retail store inventory.

www.nodia.in

Downloaded from www.pdf.tube

# CHAPTER 02
# Introduction to Computing Systems

**May/June 2018**

**1.** Who proposed the concept of the stored program in 1946, enabling instructions to be stored in memory along with data?
(A) Charles Babbage
(B) Satya Nadella
(C) Gordon Moore
(D) John Von Neumann

**Oct/Nov 2012**

**2.** In server virtualization, what does the concept of 'consolidation ratio' refer to?
(A) The ratio of physical servers to the amount of hazardous waste produced.
(B) The percentage of bandwidth consumed by multiple operating systems traversing the network.
(C) The number of virtual servers that can run on a single physical host machine.
(D) The amount of physical floor space saved by using desktop virtualization instead of physical desktops.

**May/June 2006**

**3.** What is the fundamental definition of grid computing?
(A) A computing model where multiple dumb terminals are connected to a central mainframe.
(B) A system where physical client devices are isolated from the host operating system.
(C) A network sharing many computers' resources simultaneously to solve a single problem.
(D) A technique where large numbers of similar transactions are processed in a batch sequence.

**Oct/Nov 2025**

**4.** Which statement correctly identifies a limitation inherent to hardware virtualization?
(A) Virtualization completely eliminates the need for software security provisions in a network.
(B) The consolidation ratio is limited to a maximum of 10 virtual servers per physical host.
(C) An application must traverse two operating systems, increasing processing time and overhead.
(D) Virtualization prevents the loading of older operating systems like Solaris onto new hardware.

**May/June 2021**

**5.** In computerized data processing, what distinguishes a master file from a transaction file?
(A) A master file contains temporary data, while a transaction file holds permanent records.
(B) A master file holds permanent records, while a transaction file stores periodic updates.
(C) A master file is used in batch processing, while a transaction file is for OLTP only.
(D) A master file cannot be updated, while a transaction file is continuously overwritten.

**Oct/Nov 2007**

**6.** Which statement is correct regarding analogue computers?
(A) They calculate directly with numbers expressed as digits in binary systems for accuracy.
(B) They measure continuous physical magnitudes and provide approximate results.
(C) They are exclusively used for business data processing like payroll operations in firms.
(D) They were first introduced during the fifth generation of computers for AI processing.

**May/June 2015**

**7.** What is the precise definition of an algorithm as applied to a computer processing data?
(A) A physical component of a hardware machine designed to execute specific business tasks.
(B) A finite sequence of instructions followed to

NODIA

solve a problem or process data.
(C) A continuous measurement of physical magnitudes that are analogous to digital numbers.
(D) A centralized database management system that locks records during simultaneous access.

**Oct/Nov 2019**

**8.** How do real-time systems conceptually differ from standard on-line systems?
(A) Real-time systems process data sequentially, while on-line systems process it randomly.
(B) Real-time systems exercise control during operation where delays cause critical failure.
(C) Real-time systems accept random input but process it in scheduled, optimized batches.
(D) Real-time systems do not require checkpoints or transaction logs for system recovery.

**May/June 2011**

**9.** Which of the following statements correctly identifies a characteristic of grid computing?
(A) It is restricted solely to the network of computer workstations within one corporate office.
(B) It applies the resources of multiple networked computers to solve one problem at once.
(C) It is identical to cluster computing but does not require any software to divide a program.
(D) It typically utilizes a single mainframe computer connected to dumb terminals.

**Oct/Nov 2010**

**10.** Fourth Generation computers saw the arrival of Very Large Scale Integrated Circuits (VLSI). Approximately how many transistors does a VLSI chip hold?
(A) 10 transistors
(B) 100 transistors
(C) 50000 transistors
(D) Millions of components

**May/June 2024**

**11.** Which of the following correctly describes Desktop Virtualization?
(A) It involves running multiple operating systems simultaneously on a user's local mobile device.
(B) It utilizes a single application traversing three distinct operating systems to process graphics.
(C) It requires the desktop to operate solely in an offline mode without network connectivity.
(D) It separates the user's physical device from the OS, storing data on a remote server.

**Oct/Nov 2014**

**12.** How is a hybrid computer defined?
(A) A machine operating exclusively on characters expressed as binary digits for scientific use.
(B) A computing environment integrating on-premise private clouds with hosted public clouds.
(C) A computer combining the features and capabilities of digital and analogue machines.
(D) A computer leveraging the resources of many machines in a network for parallel tasks.

**May/June 2019**

**13.** What is meant by the 'utility computing model' adopted by many cloud computing offerings?
(A) Customers pay for computing resources based on usage, similar to electricity billing.
(B) Customers purchase and own the hardware but rent the software applications monthly.
(C) Customers are required to engineer their infrastructure for peak loads in advance.
(D) Customers share computing infrastructure strictly within organizations of one community.

**Oct/Nov 2005**

**14.** Why is computational speed highly critical in scientific applications compared to general business applications?
(A) Because scientific applications involve large storage for millions of customer records.
(B) Because scientific applications require constant real-time manual manual intervention.
(C) Because scientific tasks involve low I/O volume but require complex computations.
(D) Because scientific applications utilize dumb terminals connected to a central processor.

Click Here to Buy book on Amazon

May/June 2020

**15.** Which of the following statements correctly relates to the generation of computers and their memory technologies?
(A) In the first generation, semi-conductor memories replaced magnetic core memories.
(B) In the third generation, magnetic disk storage was completely abandoned for tape.
(C) In the fourth generation, vacuum tubes were integrated into VLSI chips for memory.
(D) In the second generation, magnetic core storage was used to build large RAM systems.

Oct/Nov 2024

**16.** How is data processing fundamentally defined in the context of business administration?
(A) The systematic capture, storage, and transformation of facts into useful information.
(B) The physical design of complex three-dimensional objects using geometric calculations.
(C) The measurement of continuous physical magnitudes like varying temperature or pressure.
(D) The conversion of network protocols across incompatible machines at geographical sites.

May/June 2014

**17.** Which of the following correctly describes Software as a Service (SaaS)?
(A) It provides a full software application hosted on the cloud via a pay-per-use model.
(B) It involves offering hardware-related services using the principles of cloud computing.
(C) It involves offering a development platform on the cloud for engineers to build applications.
(D) It is a stripped-down server computer with a modular design optimized to save physical space.

Oct/Nov 2017

**18.** According to the designs for Charles Babbage's Analytical Engine, how long was it estimated to take to multiply two numbers?
(A) 2800 milliseconds
(B) 60 additions a minute
(C) 200 milliseconds
(D) 1 million instructions per second

May/June 2022

**19.** What is the underlying concept of 'Green Computing'?
(A) Utilizing obsolete hardware parts to build new specialized analogue computer systems.
(B) Developing algorithms that operate exclusively in natural languages for human use.
(C) Ensuring all data centers are powered strictly by renewable solar energy sources.
(D) Reducing energy usage and hazardous waste by replacing physical servers with virtual ones.

Oct/Nov 2008

**20.** What is the concept of 'Record Locking' in on-line transaction processing (OLTP)?
(A) It prevents simultaneous updates by locking a record while it is being modified.
(B) It prevents the system from processing any data until a complete batch is formed.
(C) It restricts the capacity of the primary storage unit to handle complex programs.
(D) It securely archives the master file at the end of every business day for recovery.

May/June 2007

**21.** Which of the following correctly describes a 'Blade Server'?
(A) A server equipped with multiple redundant power supplies taking up maximum floor space.
(B) A software application used for executing batch processing on a central mainframe.
(C) A modular, stripped-down server designed to minimize physical space and energy usage.
(D) A dumb terminal used in early timesharing systems to access a central processor.

Oct/Nov 2016

**22.** According to the design of Charles Babbage's 'Analytical Engine' in 1837, what was its planned computational speed?
(A) 1 million instructions per second
(B) 60 additions a minute
(C) 200 milliseconds to add two digits
(D) 2800 milliseconds to multiply

Downloaded from www.pdf.tube

May/June 2013

**23.** What is the conceptual difference between 'data' and 'information'?
(A) Data provides specific meaning to users, whereas information consists of raw facts.
(B) Data requires a transaction file, whereas information requires a static master file.
(C) Data is processed by analogue systems, while information is processed by digital ones.
(D) Data refers to raw meaningless facts, while information conveys meaning based on facts.

Oct/Nov 2013

**24.** Which of the following statements correctly describes a Hybrid Cloud?
(A) It is hosted by a third party and exclusively used by one specific organization.
(B) It involves sharing computing infrastructure between organizations of the same community.
(C) It provides a development platform on the cloud that is not compatible with other vendors.
(D) It combines private clouds for sensitive data with public clouds for standard workloads.

May/June 2009

**25.** Which conceptual approach does cluster computing use to help an enterprise achieve 99.999% availability?
(A) Using a single, powerful mainframe to process all transactions in a sequential order.
(B) Linking computers and devices to appear to external users as a single available system.
(C) Farming out program pieces to unused personal computers globally over the internet.
(D) Stripping down server computers to modular designs to minimize space and energy use.

Oct/Nov 2009

**26.** In a computerized environment, what does the term 'hardware' strictly refer to?
(A) The finite sequence of algorithms used to solve complex problems.
(B) The instructions that tell the machine what to do.
(C) The data records stored on secondary storage devices.
(D) The physical components of which a computer is made up.

NODIA

May/June 2023

**27.** Which of the following is a correct statement regarding Distributed Data Processing?
(A) Communication costs are reduced as most processing occurs on local on-site computers.
(B) A central processor switches from one dumb terminal to another in allocated time-slices.
(C) It eliminates the need for any communication network between computers in a system.
(D) If the main computer fails, all terminals at remote locations must suspend their operations.

Oct/Nov 2018

**28.** In real-time systems, how frequently are checkpoints typically provided to facilitate audit and recovery in case of failure?
(A) Every two to three minutes
(B) Every fraction of a millisecond
(C) Once every hour
(D) At the end of the business day

May/June 2017

**29.** Which of the following statements correctly describes a feature of Third Generation computers?
(A) High-speed vacuum tube switching devices were introduced for basic processing.
(B) Magnetic core memories completely replaced semi-conductor memories in systems.
(C) Germanium transistors were replaced by Silicon transistors and Integrated Circuits.
(D) They introduced the concept of quantum computing for complex mathematical tasks.

Oct/Nov 2023

**30.** In on-line processing systems, what is the conceptual purpose of 'rollback' and 'roll forward'?
(A) To convert physical network parts into virtual networks (VLANs) for better security.
(B) To group similar transactions together for sequential processing outside business hours.
(C) To lock a record so that no other user can update it simultaneously during a session.
(D) To restore a file to its state before an update

or re-apply changes after a failure.

**May/June 2008**

**31.** Which of the following is an INCORRECT statement about the limitations of virtualization?
(A) Virtualization introduces additional overheads and inefficiencies.
(B) Each operating system takes space in memory, which is a highly constrained resource.
(C) The duplicate OS consumes disk space but does not need to be licensed separately.
(D) Dependence on a single-point-of-failure should be addressed before deployment.

**Oct/Nov 2021**

**32.** Which of the following is NOT a stated benefit of server virtualization?
(A) Savings in floor space index
(B) Total elimination of the need for operating systems
(C) Savings in electrical consumption
(D) Improvement in profitability

**May/June 2010**

**33.** Identify the INCORRECT statement about On-Line Transaction Processing (OLTP).
(A) The transaction should immediately update the master files.
(B) The transaction file must always be sorted in the same order as the master file before updating.
(C) Validation of an item takes place before it gets stored on the secondary storage device.
(D) It requires software security provisions to prevent tampering with data.

**Oct/Nov 2015**

**34.** What is the most significant disadvantage of centralized timesharing systems?
(A) They require complex network protocols to maintain.
(B) They process data significantly faster than modern distributed systems, causing buffer overflows.
(C) They allow unauthorized users to update records simultaneously without record locking.
(D) The failure of the main computer causes all remote terminals to suspend operations.

**May/June 2025**

**35.** Which of the following was NOT an advantage or characteristic of Second Generation computers compared to First Generation?
(A) Integration of artificial intelligence and natural language processing techniques.
(B) Use of transistors which were highly reliable compared to vacuum tubes.
(C) Dissipation of one tenth of the heat of tubes.
(D) Occupation of one tenth of the space of tubes.

**Oct/Nov 2006**

**36.** What is the defining characteristic of Fifth Generation computers?
(A) They use intelligent programming and artificial intelligence to interpret natural languages.
(B) They use silicon transistors and magnetic core storage.
(C) They are strictly limited to quantum computing technology.
(D) They rely exclusively on centralized dumb terminals.

**May/June 2016**

**37.** Which of the following is an INCORRECT statement regarding the components of Charles Babbage's Analytical Engine?
(A) The CONTROL UNIT converted continuous physical magnitudes into numerical indications.
(B) The STORE was meant to hold numbers and store intermediate results.
(C) The ARITHMETIC UNIT was called the 'mill' and performed arithmetical operations through rotations of gears and wheels.
(D) It included an INPUT DEVICE to enter numbers and instructions.

**Oct/Nov 2022**

**38.** Which of the following is NOT an element typically associated with On-Line Enquiries?
(A) Macros
(B) Structured Query Language (SQL)
(C) Fourth Generation Language (4GL)
(D) Magnetic Ink Character Recognition (MICR) reader/sorter

**May/June 2005**

**39.** What is the best reason why banking accounting systems have extensively used batch processing for tasks like interest calculations?

Click Here to Buy book on Amazon

(A) Interest calculations require immediate online response to customers.
(B) Batch processing is inherently more secure against hacking than real-time processing.
(C) Batch processing allows transactions to immediately update the master files one by one.
(D) These routines occur after business hours and do not require high-cost online processing.

**Oct/Nov 2011**

**40.** Identify the INCORRECT statement regarding cloud computing service models and major players.
(A) Amazon Web Services (AWS) offers Amazon Elastic Compute Cloud, known as EC2.
(B) Salesforce.com is a pioneer in the SaaS sector, offering Customer Relationship Management (CRM) applications.
(C) Microsoft's online services include Office Live and Exchange Online.
(D) Google App Engine serves as an IaaS requiring high initial fees for data storage.

**May/June 2012**

**41.** Arrange the following computer hardware technologies in the chronological order of their primary use across computer generations:
I Microprocessor chip (VLSI)
II Vacuum tube switching devices
III Transistors (Germanium/Silicon)
IV Ultra Large Scale Integrated (ULSI) chips
V Integrated Circuits (ICs)
(A) II, V, III, I, IV
(B) II, III, V, I, IV
(C) III, II, V, IV, I
(D) II, III, I, V, IV

**Oct/Nov 2020**

**42.** Which of the following is an INCORRECT statement regarding the benefits of Cloud Computing?
(A) It increases utilization by delivering resources only for as long as those resources are needed.
(B) It allows for rapid scalability and increased efficiency.
(C) It requires companies to expand procurement processes and duplicate administrative skills.
(D) It offers a high level of redundancy and backup at a low cost.

**May/June 2023**

**43.** Which of the following is NOT an example of Software as a Service (SaaS)?
(A) Google's Gmail
(B) Amazon Elastic Compute Cloud (EC2)
(C) Microsoft's Hotmail
(D) Salesforce.com CRM

**Oct/Nov 2017**

**44.** Which of the following is NOT an application or component generally associated with Fourth Generation computers?
(A) Graphical User Interfaces (GUIs)
(B) Microprocessor chip
(C) Personal Computers (PCs)
(D) Germanium transistors

**May/June 2005**

**45.** In the context of the utility computing model, what does sharing "perishable and intangible" computing power between multiple tenants achieve?
(A) It reduces utilization rates and increases server idle times.
(B) It ensures that software must be licensed separately for each virtual machine.
(C) It improves utilization rates, reduces costs, and increases application development speed.
(D) It guarantees zero latency for all geographical locations globally.

**Oct/Nov 2009**

**46.** Which of the following is an INCORRECT statement regarding Batch Processing?
(A) Transactions are grouped together and processed sequentially at once without interruption.
(B) Transaction data is fed into storage under CPU control without requiring prior sorting.
(C) Transaction items are matched against the master item, and the master item is changed accordingly.
(D) It utilizes technological resources very effectively, especially where a large number of transactions are involved.

**May/June 2016**

**47.** What is the primary purpose of Grid Engine software as provided by Sun Microsystems?
(A) To host web pages securely in an extranet

NODIA

environment.
(B) A tool allowing engineers to pool computer cycles across workstations for management.
(C) To strictly provision virtual servers for legacy applications.
(D) To lock records during online transaction processing.

**Oct/Nov 2008**

**48.** Which of the following statements about grid computing is INCORRECT?
(A) Grid computing can be confined to the network of computer workstations within a single corporation.
(B) In all grid architectures, computers must be managed by a single central mainframe system.
(C) It requires the use of software that can divide and farm out pieces of a program.
(D) The SETI@home project is a well-known example of grid computing in the public domain.

**May/June 2018**

**49.** Which of the following companies is NOT an alternative software and systems provider to VMware in virtualization?
(A) Apple
(B) Citrix
(C) IBM
(D) HP

**Oct/Nov 2024**

**50.** Which of the following is NOT a step involved in how Batch Systems work?
(A) Documents are sorted by type to form separate batches.
(B) Each batch is given a header consisting of batch number, type, and number of documents.
(C) Transaction items are stored on secondary storage under CPU control without prior sorting.
(D) A new copy of the master file is created reflecting the changes from the transaction file.

**May/June 2022**

**51.** What was the primary objective of the ENERGY STAR program launched by the U.S. Environmental Protection Agency?
(A) To enforce mandatory limits on where financial institutions can store data.
(B) To mandate the use of blade servers in all data centers.
(C) To standardize the speed of internet bandwidth globally.
(D) To promote and recognize energy-efficiency in monitors and consumer electronics.

**Oct/Nov 2014**

**52.** Which of the following is an INCORRECT statement concerning the challenges of cloud computing?
(A) Budgeting the cost of on-demand services can be difficult without comparable benchmarks.
(B) Delivering intensive and complex data over the network requires sufficient bandwidth, which can be costly.
(C) Hacking can affect multiple clients even if only one site is attacked, resulting in collateral damage.
(D) Physical distance between a data centre and a data entry point has no impact on performance.

**May/June 2007**

**53.** Which of the following is NOT one of the five basic units of today's electronic computer?
(A) Arithmetic & Logic Unit (ALU)
(B) Control Unit
(C) Millimeter Wave Unit
(D) Memory Unit

**Oct/Nov 2012**

**54.** Which of the following provides the best description of a Hybrid Cloud?
(A) A cloud exclusively built for a consortium of universities.
(B) A computing platform deployed internally but hosted globally without network restrictions.
(C) A setup where an organization uses private clouds for sensitive data and public clouds for scaling.
(D) A cloud where infrastructure is fully hosted by a third party with no visibility to the customer.

**May/June 2015**

**55.** Which of the following is NOT considered a challenge of cloud computing?
(A) The inability to provision or de-provision

Downloaded from www.pdf.tube

servers dynamically based on demand.
(B) Security and Privacy (Collateral damage)
(C) Bandwidth Cost for data-intensive applications
(D) Latency impacting core banking operations

**Oct/Nov 2020**

**56.** Which of the following is an INCORRECT statement regarding Real-Time Systems?
(A) They are static environments, making them very easy to audit and recover after a failure.
(B) They accept random input at random time intervals, causing the status of files to change dynamically.
(C) Checkpoints are typically provided for every two to three minutes in these systems.
(D) Any delay beyond a specific time in exercising control would be disastrous.

**May/June 2011**

**57.** What is the primary benefit of cloud computing with respect to business continuity for banking firms?
(A) Increased fault tolerance, data protection, and redundancy provided at a lower cost.
(B) Complete elimination of the need for data encryption.
(C) Immediate reduction of data residency and ownership issues.
(D) Reduction in the physical distance between the data centre and data entry point.

**Oct/Nov 2005**

**58.** Which of the following statements regarding computing environments is INCORRECT?
(A) Cloud apps are accessible only via isolated LANs that are disconnected from the Internet.
(B) The goal of fifth-generation computing is to develop devices that respond to natural language input.
(C) Fourth-generation computers saw the decentralization of computer organization and emergence of networks.
(D) Centralized processing uses dumb terminals attached to a central mainframe.

**May/June 2019**

**59.** What is the most appropriate description of the 'mill' in Charles Babbage's Analytical Engine?
(A) A component designed exclusively to check the correctness of sequence of operations.
(B) A system to display final results on a punch card.
(C) A device performing arithmetical operations on numbers using rotations of gears.
(D) A continuous physical magnitude measuring device.

**Oct/Nov 2017**

**60.** Which of the following is NOT a characteristic of analogue computers?
(A) They deal with quantities that continuously vary.
(B) They provide highly accurate results expressed in binary digits for financial billing.
(C) They are often used for scientific and engineering purposes.
(D) They measure continuous physical magnitudes like voltage and temperature.

NODIA

**May/June 2013**

**61.** Match the Cloud Service Models (List I) with their definitions (List II).
List I: (Service Model)
P. IaaS
Q. PaaS
R. SaaS
S. BPOS
List II: (Definition)
1. Complete software offering accessed on a pay-per-use basis (e.g., Salesforce CRM).
2. Hardware related services like database, disk storage, or virtual servers.
3. Microsoft's online version of Office Suite.
4. Development platform provided on the cloud for engineers to build upon.
(A) P-4, Q-2, R-3, S-1
(B) P-2, Q-1, R-4, S-3
(C) P-2, Q-4, R-1, S-3
(D) P-1, Q-3, R-2, S-4

**Oct/Nov 2013**

**62.** Consider the following statements regarding cluster computing:
I A common use of cluster computing is to load balance traffic on high-traffic Web sites.
II To the outside world, a cluster of multiple computers appears to be a single system.
Which of the above statement(s) is/are correct?
(A) Only (I)
(B) Only (II)

(C) Both (I) and (II)
(D) Neither (I) nor (II)

**May/June 2006**

**63.** Match the Computer Generations (List I) with their key technological features (List II).
List I: (Generation)
P. First Generation
Q. Second Generation
R. Third Generation
S. Fourth Generation
List II: (Technology)
1. Microprocessor chip (VLSI)
2. Vacuum tube switching devices
3. Transistors and magnetic core storage
4. ICs replacing discrete transistors
(A) P-2, Q-3, R-4, S-1
(B) P-2, Q-4, R-3, S-1
(C) P-3, Q-2, R-4, S-1
(D) P-1, Q-3, R-4, S-2

**Oct/Nov 2016**

**64.** Consider the following statements regarding the benefits of cloud computing:
I It forces enterprises into a rigid structure with increased downtime on IT changes.
II It accelerates and fosters the adoption of innovations by alleviating the need to physically find hardware resources.
III It improves resource utilization by pooling resources into large clouds.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II) and (III)

**May/June 2025**

**65.** Identify the correctly matched pair regarding computer generations and their defining technologies.
(A) Second Generation — Magnetic core storage and Transistors
(B) First Generation — Integrated Circuits (ICs)
(C) Third Generation — Microprocessor chips and VLSI
(D) Fourth Generation — Vacuum tube switching devices

**Oct/Nov 2023**

**66.** Consider the following statements regarding Grid Computing:
I It applies the resources of many computers in a network to a single problem simultaneously.
II The SETI@home project is a prominent example of public domain grid computing.
III It requires software to divide and farm out pieces of a program.
IV It cannot be confined to the network of computer workstations within a single corporation.
Which combination of statements is correct?
(A) (I), (II), and (III) only
(B) (I), (II), and (IV) only
(C) (II), (III), and (IV) only
(D) (I), (II), (III), and (IV)

**May/June 2014**

**67.** Arrange the evolution of data processing systems in the correct chronological order:
I Distributed processing via communication networks
II Mainframe computers with dumb terminals
III Grid and Cloud computing
IV Decentralized processing using mini and micro-computers
(A) II, I, IV, III
(B) IV, II, I, III
(C) II, IV, I, III
(D) I, II, IV, III

**Oct/Nov 2018**

**68.** Consider the following statements regarding the history of computers:
I Charles Babbage designed the 'Analytical Engine' in 1837 to perform mathematical problems at a speed of 60 additions a minute.
II John Von Neumann introduced the stored program concept in 1946, allowing instructions and data to reside in memory.
Which of the above statement(s) is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**May/June 2020**

**69.** Consider the following statements regarding general-purpose vs. special-purpose computers:
I Special-purpose machines have a built-in set of instructions permanently dedicated to one specific task.
II Scientific applications typically involve a

Click Here to Buy book on Amazon

huge volume of input data and output lines, with very slow computational speeds.

III Business applications like credit card billing involve thousands of customers and require large storage capacity.

Which of the above statement(s) is/are correct?

(A) (I) and (II) only
(B) (I) and (III) only
(C) (II) and (III) only
(D) (I), (II) and (III)

**Oct/Nov 2009**

**70.** Match the Virtualization Concepts (List I) with their corresponding descriptions (List II).

List I: (Concept)

P. Server Virtualization
Q. Desktop Virtualization
R. Blade Server
S. VSANs

List II: (Description)

1. Separation of physical client device from the operating system for remote access.
2. Running multiple isolated OS environments side by side on a single physical machine.
3. Virtualization of storage areas offering greater flexibility and reduced redundancy.
4. A stripped-down server with modular design optimizing physical space and energy.

(A) P-1, Q-2, R-3, S-4
(B) P-2, Q-4, R-1, S-3
(C) P-2, Q-1, R-4, S-3
(D) P-4, Q-3, R-2, S-1

**May/June 2008**

**71.** Consider the following statements comparing Data Processing models:

I In batch processing, items are matched against the master item after being sorted.

II In OLTP, transaction data is directly fed into the secondary storage under CPU control without sorting.

III Batch processing is typically used in accounting systems for non-urgent tasks like interest calculation.

IV SQL and 4GL are typically used to construct queries against data updated in batch mode.

Which combination is correct?

(A) (I), (II), (III), and (IV)
(B) (I), (II), and (III) only
(C) (I), (II), and (IV) only
(D) (II), (III), and (IV) only

NODIA

**Oct/Nov 2011**

**72.** Match the Data Processing Methods (List I) with their operational characteristics (List II).

List I: (Method)

P. Batch Processing
Q. OLTP
R. Real-Time Systems
S. Distributed Processing

List II: (Characteristic)

1. Transactions directly feed into storage and immediately update master records.
2. Computers connected by a network share workload and resources globally.
3. Transactions grouped and sorted before updating master files sequentially.
4. Control exercised during actual functioning; checkpoints every 2-3 minutes.

(A) P-1, Q-3, R-2, S-4
(B) P-3, Q-1, R-4, S-2
(C) P-3, Q-4, R-1, S-2
(D) P-2, Q-1, R-4, S-3

**May/June 2010**

**73.** Consider the following statements regarding On-Line Transaction Processing (OLTP):

I Transaction validation takes place after it is permanently written to the master file.

II Record locking is provided so that a record under use cannot be updated by someone else at the same time.

Which of the above statement(s) is/are correct?

(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**Oct/Nov 2025**

**74.** Identify the correctly matched pair regarding data processing models and their common applications.

(A) Batch Processing — Airline ticket reservations
(B) OLTP — Off-hours calculation of bank account interest
(C) Real-Time System — Front-office counter terminals and dealer support systems
(D) Centralized Processing — Peer-to-peer sharing of processing power (SETI@home)

**May/June 2024**

**75.** Consider the following statements regarding Distributed Data Processing:

I It facilitates quick access to data especially when distance is a major factor.
II Communication costs are generally higher than centralized systems due to local processing.
III Users must be careful about maintaining confidentiality and integrity of programs and data files.
IV Users may have to convert protocols if machines at different sites are incompatible.
Which combination of statements is correct?
(A) (I), (II), and (IV) only
(B) (I), (III), and (IV) only
(C) (II), (III), and (IV) only
(D) (I), (II), (III), and (IV)

**Oct/Nov 2021**

**76.** Match the components of Charles Babbage's Analytical Engine (List I) with their corresponding functions (List II).
List I: (Component)
P. STORE
Q. Mill
R. CONTROL UNIT
S. INPUT DEVICE
List II: (Function)
1. To check the correctness of sequence of operations.
2. To enter numbers and instructions.
3. To hold numbers and intermediate results.
4. To perform arithmetical operations automatically.
(A) P-4, Q-3, R-2, S-1
(B) P-3, Q-1, R-4, S-2
(C) P-2, Q-4, R-1, S-3
(D) P-3, Q-4, R-1, S-2

**May/June 2012**

**77.** Consider the following statements regarding Real-Time Systems:
I They are dynamic in nature, accepting random input at random time intervals.
II Due to constant file changes, checkpoints are provided for every two to three minutes.
III Counter terminals in branches are a common example of front-office systems using real-time technology.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II) and (III)

**Oct/Nov 2006**

**78.** Match the Cloud Computing Providers (List I) with their respective product/service (List II).
List I: (Provider)
P. Amazon
Q. Google
R. Microsoft
S. Sun Microsystems
List II: (Service)
1. App Engine
2. Elastic Compute Cloud (EC2)
3. Project Caroline / Network.com
4. Azure / Dynamics CRM Online
(A) P-1, Q-2, R-3, S-4
(B) P-2, Q-4, R-1, S-3
(C) P-4, Q-1, R-2, S-3
(D) P-2, Q-1, R-4, S-3

NODIA

**May/June 2021**

**79.** Consider the following statements regarding Virtualization and Green Computing:
I Virtualization reduces hardware costs but significantly increases electrical consumption.
II The U.S. Environmental Protection Agency launched the ENERGY STAR program to promote energy-efficiency.
Which of the above statement(s) is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**Oct/Nov 2019**

**80.** Identify the INCORRECTLY matched pair regarding the functioning of OLTP systems.
(A) Rollback — Restoring the master to its original position before an update
(B) Roll forward — Re-applying updates to an earlier copy
(C) Record Locking — Preventing multiple people from updating the same record simultaneously
(D) Check pointing — Grouping all daytime transactions for processing at midnight.

**May/June 2017**

**81.** Consider the following statements regarding the limitations of hardware virtualization:
I A single application has two operating systems to traverse, leading to more

processing overhead.
II Each OS takes up memory, which is highly constrained on any server.
III The duplicate OS consumes disk space and must be licensed separately.
IV It entirely eliminates the risk of a single-point-of-failure.
Which combination of statements is correct?
(A) (I), (II), and (IV) only
(B) (I), (III), and (IV) only
(C) (I), (II), and (III) only
(D) (II), (III), and (IV) only

**Oct/Nov 2015**

**82.** Match the Cloud Location Models (List I) with their characteristics (List II).
List I: (Model)
P. Public Cloud
Q. Private Cloud (On-premise)
R. Hybrid Cloud
S. Community Cloud
List II: (Characteristic)
1. Uses a mix of internal deployments and external vendor setups based on scaling/security needs.
2. Infrastructure hosted by vendor, shared among any organization with no customer visibility into location.
3. Infrastructure shared among organizations with similar backgrounds (e.g., government entities).
4. Infrastructure dedicated strictly to one organization and hosted internally.
(A) P-2, Q-4, R-1, S-3
(B) P-2, Q-4, R-3, S-1
(C) P-4, Q-2, R-1, S-3
(D) P-1, Q-3, R-2, S-4

**May/June 2023**

**83.** Match the following elements of computer technology (List I) with their correct operational context (List II).
List I: (Element)
P. Macro
Q. Protocol
R. MICR
S. ENERGY STAR
List II: (Context)
1. Set of rules governing the network in distributed systems.
2. Voluntary labelling program to promote energy efficiency.
3. Reader/sorter used for splitting cheques into batches.
4. Set of instructions to perform repetitive tasks in online queries.
(A) P-1, Q-4, R-2, S-3
(B) P-4, Q-2, R-3, S-1
(C) P-3, Q-1, R-4, S-2
(D) P-4, Q-1, R-3, S-2

**Oct/Nov 2022**

**84.** Consider the following statements regarding the batch system for cheque-clearing in banks:
I Cheques include codes written with magnetic ink.
II A MICR reader/sorter reads the codes and sorts the cheques in order.
III The amount owed and collected is settled through accounts at the central bank after details are exchanged.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II) and (III)

**May/June 2005**

**85.** Consider the following statements regarding file types in batch processing:
I A master file is temporary in nature and typically contains data like hours worked in a month.
II A transaction file contains permanent details like employee name, address, and income tax code.
Which of the above statement(s) is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**Oct/Nov 2010**

**86.** Match the Computer classifications (List I) with their descriptions (List II).
List I: (Computer Type)
P. Analogue
Q. Digital
R. Hybrid
S. Special-purpose
List II: (Description)
1. Dedicated to one specific task, highly efficient but lacks versatility.
2. Measures continuous physical magnitudes,

Downloaded from www.pdf.tube

# STUDYING FROM PDFs?

# THINK AGAIN.

If you are studying only from PDFs,
you are wasting valuable time.

Research shows that learning from

**PRINTED BOOKS** has up to

**4× HIGHER RETENTION**

than studying from screens.

**PRINT BOOK = BETTER MEMORY**

**PDF = LOWER RETENTION**

Those who study from **PRINTED BOOKS**
move **AHEAD.**

Others are left **BEHIND**
in competition.

In competitive exams,
being average is not enough.

## STAY ONE STEP AHEAD.

giving approximate results.
3. Operates on numbers/characters expressed as digits, providing accurate results.
4. Combines desirable features to simulate systems like guided missiles.

(A) P-3, Q-2, R-4, S-1
(B) P-2, Q-3, R-4, S-1
(C) P-2, Q-3, R-1, S-4
(D) P-4, Q-3, R-2, S-1

**May/June 2009**

**87.** Consider the following statements regarding cloud computing service models:
I IaaS involves offering hardware-related services like database or disk storage.
II PaaS platforms provided by different vendors are typically highly compatible with each other.
III SaaS includes applications like Salesforce.com and Google's Gmail.
IV Cloud applications use large data centers and powerful servers to host web services.
Which combination of statements is correct?
(A) (I), (II), and (III) only
(B) (I), (III), and (IV) only
(C) (II), (III), and (IV) only
(D) (I), (II), (III), and (IV)

**Oct/Nov 2007**

**88.** Match the Cloud Computing Challenges (List I) with their descriptions (List II).
List I: (Challenge)
P. Latency
Q. Residency of data
R. Collateral damage
S. Bandwidth Cost
List II: (Description)
1. Expense incurred to deliver intensive and complex data over the network.
2. Impact on performance due to physical distance causing delays in operations.
3. Regulatory compliances imposing government-mandated limits on storage locations.
4. Hacking attacks affecting multiple clients even if only one site is initially breached.

(A) P-3, Q-2, R-1, S-4
(B) P-2, Q-3, R-4, S-1
(C) P-2, Q-1, R-4, S-3
(D) P-4, Q-3, R-2, S-1

**May/June 2016**

**89.** Consider the following statements regarding computer generations:
I Third-generation computers witnessed the use of ICs consisting of transistors, resistors, and capacitors on a single chip.
II Fourth-generation computers saw the emergence of extremely powerful PCs, computer networks, and GUIs.
III Fifth-generation computers rely on vacuum tubes for natural language processing.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II) and (III)

**Oct/Nov 2008**

**90.** Identify the INCORRECTLY matched pair regarding cloud computing terminology.
(A) IaaS — Offering a development platform strictly without virtual servers.
(B) Public Cloud — Infrastructure hosted by vendor, shared between any organizations
(C) SaaS — Users access software applications like Gmail hosted by vendor on pay-per-use
(D) Hybrid Cloud — Deployment involving both private and public clouds

**May/June 2018**

**91.** The following questions consist of two statements – Assertion (A) and Reason (R). Answer these questions selecting the appropriate option.
Assertion (A): In third generation computers, magnetic core memories were replaced by semi-conductor memories.
Reason (R): Germanium transistors were replaced by Silicon transistors, allowing ICs to hold multiple components on a single chip.
(A) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2024**

**92.** Read the following case study and answer the questions that follow.
*Bank Beta historically used a single large*

NODIA

*mainframe located at its head office to process all branch data via 'dumb terminals.' Due to operational delays when the mainframe crashed, management decided to switch to a system where branches use their own computers linked via a communication network, sharing workload and software resources.*

The historical setup used by Bank Beta, where one processor allocated time-slices to dumb terminals, is known as:

(A) Distributed data processing
(B) Virtualized server environment
(C) Timesharing system
(D) Peer-to-peer computing

**May/June 2022**

**93.** Consider the following statements about the benefits of Virtualization:

I It reduces hardware costs by running multiple operating systems on the same physical server.
II Manageability becomes convenient as resources are available at a single point.
III It eliminates the need for software licenses for the duplicated OS.
IV It provides high Return on Investment (ROI) by improving the consolidation ratio.
V It leads to savings in floor space index and electrical consumption.

Which combination of statements is correct?

(A) (I), (II), (III), and (V)
(B) (II), (III), (IV), and (V)
(C) (I), (II), (IV), and (V)
(D) (I), (III), (IV), and (V)

**Oct/Nov 2014**

**94.** Read the following case study and answer the questions that follow.

*Bank Gamma is adopting cloud technology. It decides to host its highly sensitive core banking database internally on its own infrastructure to meet regulatory standards. However, for its customer-facing mobile application and non-critical CRM software, it decides to rent computing power from Amazon Web Services (AWS) to save costs.*

By using AWS for its customer-facing mobile application, Bank Gamma takes advantage of the "utility computing model". What does this imply?

(A) Bank Gamma purchases the hardware from Amazon permanently.
(B) Bank Gamma engineers its local hardware to withstand peak loads of the mobile app.
(C) Bank Gamma is billed for usage, avoiding capital expenditure on hardware.
(D) Bank Gamma shares its database credentials with Amazon engineers.

**May/June 2007**

**95.** The following questions consist of two statements – Assertion (A) and Reason (R). Answer these questions selecting the appropriate option.

Assertion (A): Some experts consider that private clouds are not real examples of cloud computing.

Reason (R): The computing infrastructure in a private cloud is dedicated to a particular organization and not shared with other organizations.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2012**

**96.** Read the following case study and answer the questions that follow.

*Bank Delta currently runs 800 physical UNIX and Linux servers spread across its data centers. This has led to massive hardware, power, and maintenance costs. The bank's IT head proposes implementing software from VMware to consolidate these down to 60 physical machines, where each physical machine will run multiple operating systems side by side.*

Which of the following represents a limitation Bank Delta must carefully analyse before deploying this solution?

(A) The inability to load older operating systems.
(B) An application must traverse two OSs, equating to slower responses and overhead.
(C) The physical floor space index will dramatically increase.
(D) They will be forced to switch back to magnetic core memory.

Click Here to Buy book on Amazon

May/June 2015

**97.** Which of the following statements correctly list the five basic functions of an electronic computer?

I Input involves the receipt of facts or data.
II Memory stores facts until needed.
III Arithmetic-Logic handles all calculations and comparisons.
IV Control interprets and executes instructions to maintain order.
V Output communicates results to users in meaningful forms.

Which combination of statements is correct?
(A) (I), (II), (III), and (IV) only
(B) (II), (III), (IV), and (V) only
(C) (I), (III), (IV), and (V) only
(D) All (I), (II), (III), (IV), and (V)

Oct/Nov 2020

**98.** Read the following case study and answer the questions that follow.
*Bank Alpha is upgrading its core computing infrastructure. The IT department handles various routines. During business hours, counter terminals answer customer inquiries immediately. After midnight, the system processes all accumulated daily interest and service charges.*
Based on the provided information, which processing method is most appropriate for Bank Alpha's midnight processing of interest and charges?
(A) Batch Processing
(B) Real-Time Processing
(C) Desktop Virtualization
(D) Grid Computing

May/June 2011

**99.** Read the following case study and answer the questions that follow.
*Bank Gamma is adopting cloud technology. It decides to host its highly sensitive core banking database internally on its own infrastructure to meet regulatory standards. However, for its customer-facing mobile application and non-critical CRM software, it decides to rent computing power from Amazon Web Services (AWS) to save costs.*
Which type of cloud deployment model is Bank Gamma using?
(A) Public Cloud strictly
(B) Hybrid Cloud
(C) Community Cloud
(D) On-premise Private Cloud strictly

Oct/Nov 2005

**100.** The following questions consist of two statements – Assertion (A) and Reason (R). Answer these questions selecting the appropriate option.
Assertion (A): Real-time systems are notoriously difficult to audit or recover in case of failure.
Reason (R): They are dynamic in nature as they accept random input at random time intervals, causing the status of files to change dynamically.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

NODIA

May/June 2019

**101.** Read the following case study and answer the questions that follow.
*The Clearing Department of a Central Bank handles millions of physical cheques daily. Each cheque has account details printed using special ink. The cheques are fed into a machine, read, sorted by settlement bank, and processed in one massive uninterrupted run to determine the net settlement amount.*
The method of grouping all cheques by settlement bank and processing them sequentially without interruption is an example of:
(A) Batch Processing
(B) On-Line Processing (OLTP)
(C) Real-Time System
(D) Grid Computing

Oct/Nov 2017

**102.** Consider the following statements about On-Line Enquiries and Systems:

I Financial organizations use them for immediate access to exchange rates and customer account statuses.
II Enquiries can only be built using macros and explicitly reject the use of SQL or 4GL.
III On-line enquiry systems can display or print the information asked by the user.
IV An on-line enquiry system typically does not perform real-time transaction processing itself.
V They can operate against data that was

updated in batch mode previously.

Which combination of statements is correct?

(A) (I), (III), (IV), and (V)
(B) (I), (II), (III), and (IV)
(C) (I), (II), (IV), and (V)
(D) (II), (III), (IV), and (V)

**May/June 2013**

**103.** Read the following case study and answer the questions that follow.

*Bank Alpha is upgrading its core computing infrastructure. The IT department handles various routines. During business hours, counter terminals answer customer inquiries immediately. After midnight, the system processes all accumulated daily interest and service charges.*

If two tellers at different branches of Bank Alpha attempt to withdraw funds from the same customer's account simultaneously, what software feature is strictly required to prevent the account balance from being inaccurately updated?

(A) Check pointing
(B) Record Locking
(C) Roll forward logging
(D) Protocol Conversion

**Oct/Nov 2013**

**104.** The following questions consist of two statements – Assertion (A) and Reason (R). Answer these questions selecting the appropriate option.

Assertion (A): In on-line processing systems, software security provisions are completely unnecessary.

Reason (R): Record locking is a software feature used to prevent multiple users from simultaneously updating the same record, thereby ensuring data consistency.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2006**

**105.** Read the following case study and answer the questions that follow.

*Bank Delta currently runs 800 physical UNIX and Linux servers spread across its data centers. This has led to massive hardware, power, and maintenance costs. The bank's IT head proposes implementing software from VMware to consolidate these down to 60 physical machines, where each physical machine will run multiple operating systems side by side.*

By consolidating 800 servers down to 60, Bank Delta significantly reduces heat generation and hazardous material disposal. This aligns directly with the goals of which concept?

(A) Cloud Residency
(B) Timesharing
(C) Green Computing
(D) Rollback Recovery

**Oct/Nov 2016**

**106.** Consider the following statements regarding challenges in cloud computing:

I Security risks include collateral damage, where an attack on one site affects multiple clients.
II Latency issues can cause delays in core banking operations like card authorization.
III SLAs provided by vendors always fully guarantee flawless availability and scalability.
IV Data residency concerns arise due to government-mandated limits on storage locations.
V Bandwidth costs can be significantly high for data-intensive applications.

Which combination of statements is correct?

(A) (I), (II), (III), and (V)
(B) (I), (II), (IV), and (V)
(C) (II), (III), (IV), and (V)
(D) (I), (III), (IV), and (V)

**May/June 2025**

**107.** Read the following case study and answer the questions that follow.

*Bank Gamma is adopting cloud technology. It decides to host its highly sensitive core banking database internally on its own infrastructure to meet regulatory standards. However, for its customer-facing mobile application and non-critical CRM software, it decides to rent computing power from Amazon Web Services (AWS) to save costs.*

If Bank Gamma decides to utilize an application offered by Salesforce.com for its Customer Relationship Management space, under which cloud service model does this fall?

Downloaded from www.pdf.tube

(A) SaaS
(B) IaaS
(C) PaaS
(D) VSAN

**Oct/Nov 2023**

**108.** The following questions consist of two statements – Assertion (A) and Reason (R). Answer these questions selecting the appropriate option.
Assertion (A): Batch processing is not appropriate for on-line transactions like railway ticket reservations.
Reason (R): Batch processing does not immediately update master files, reducing timeliness when immediate response is needed.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2014**

**109.** Read the following case study and answer the questions that follow.
*Bank Beta historically used a single large mainframe located at its head office to process all branch data via 'dumb terminals.' Due to operational delays when the mainframe crashed, management decided to switch to a system where branches use their own computers linked via a communication network, sharing workload and software resources.*
The new system adopted by Bank Beta, involving computers connected via a network handling their own workloads and sharing resources, is best defined as:
(A) Grid Computing
(B) Batch Processing
(C) Cloud Computing (IaaS)
(D) Distributed Data Processing

**Oct/Nov 2018**

**110.** The following questions consist of two statements – Assertion (A) and Reason (R). Answer these questions selecting the appropriate option.
Assertion (A): Adopting virtualization utilizing blade servers minimizes the physical space and energy used in data centers.
Reason (R): Blade servers are stripped-down server computers with a modular design that have many components removed to save space and minimize power consumption.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

NODIA

**May/June 2020**

**111.** Read the following case study and answer the questions that follow.
*The Clearing Department of a Central Bank handles millions of physical cheques daily. Each cheque has account details printed using special ink. The cheques are fed into a machine, read, sorted by settlement bank, and processed in one massive uninterrupted run to determine the net settlement amount.*
The special technology used to read the pre-printed account details and cheque numbers is known as:
(A) Check pointing
(B) Magnetic core storage
(C) Macro processing
(D) MICR (Magnetic Ink Character Recognition)

**Oct/Nov 2009**

**112.** The following questions consist of two statements – Assertion (A) and Reason (R). Answer these questions selecting the appropriate option.
Assertion (A): Desirable features of both digital and analogue computers can be combined to create a hybrid computer.
Reason (R): Special cases, such as simulating a guided missile system, require the capabilities of both computer types.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2008

**113.** The following questions consist of two statements – Assertion (A) and Reason (R). Answer these questions selecting the appropriate option.
Assertion (A): Grid computing is highly effective for solving scientific or technical problems that require a great number of processing cycles.
Reason (R): It applies the resources of many computers in a network to a single problem at the same time.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Oct/Nov 2011

**114.** Read the following case study and answer the questions that follow.
*Bank Gamma is adopting cloud technology. It decides to host its highly sensitive core banking database internally on its own infrastructure to meet regulatory standards. However, for its customer-facing mobile application and non-critical CRM software, it decides to rent computing power from Amazon Web Services (AWS) to save costs.*
The regulatory compliance requiring Bank Gamma to host sensitive data internally primarily addresses which specific challenge of cloud computing?
(A) Latency
(B) Residency of data
(C) Bandwidth cost
(D) Scalability

May/June 2010

**115.** Read the following case study and answer the questions that follow.
*Bank Alpha is upgrading its core computing infrastructure. The IT department handles various routines. During business hours, counter terminals answer customer inquiries immediately. After midnight, the system processes all accumulated daily interest and service charges.*
When a bank teller at Bank Alpha answers questions about a customer's account balance over the counter terminal, which type of processing system is the teller directly relying upon?
(A) Centralized Batch System
(B) Grid Computing Network
(C) Virtual Storage Area Network (VSAN)
(D) Front-office Real-Time System

Oct/Nov 2025

**116.** Consider the following statements regarding computer generations and processing concepts:
I First generation used vacuum tubes and took about 200 milliseconds to add.
II Second generation introduced FORTRAN and COBOL.
III Third generation increased switching speed and reliability by almost 10 times compared to transistors.
IV Fourth generation brought microprocessor chips (VLSI) holding around 50000 transistors.
V Fifth generation introduced NLP but explicitly avoids any Artificial Intelligence (AI) logic.
Which combination of statements is correct?
(A) (I), (II), (III), and (V)
(B) (I), (III), (IV), and (V)
(C) (II), (III), (IV), and (V)
(D) (I), (II), (III), and (IV)

May/June 2024

**117.** Read the following case study and answer the questions that follow.
*Bank Delta currently runs 800 physical UNIX and Linux servers spread across its data centers. This has led to massive hardware, power, and maintenance costs. The bank's IT head proposes implementing software from VMware to consolidate these down to 60 physical machines, where each physical machine will run multiple operating systems side by side.*
The technological concept the IT head is proposing is called:
(A) Grid computing
(B) Cluster computing
(C) Distributed processing
(D) Virtualization of servers

Oct/Nov 2021

**118.** The following questions consist of two statements – Assertion (A) and Reason (R). Answer these questions selecting the appropriate option.
Assertion (A): A major disadvantage of distributed data processing is that it significantly

Click Here to Buy book on Amazon

increases communication costs compared to centralized systems.
Reason (R): In distributed processing, most processing tasks are handled by local computers, which reduces the frequency and volume of data that must be transmitted over long distances.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2012**

**119.** Read the following case study and answer the questions that follow.
*Bank Beta historically used a single large mainframe located at its head office to process all branch data via 'dumb terminals.' Due to operational delays when the mainframe crashed, management decided to switch to a system where branches use their own computers linked via a communication network, sharing workload and software resources.*
When Bank Beta implements this new networked architecture, which of the following becomes a critical new challenge the bank must actively address?
(A) Maintaining program integrity while handling incompatible protocols.
(B) High communication costs compared to the mainframe system.
(C) Need for physical space for dumb terminals.
(D) Setting up magnetic core storage for each branch.

**Oct/Nov 2006**

**120.** The following questions consist of two statements – Assertion (A) and Reason (R). Answer these questions selecting the appropriate option.
Assertion (A): Moving systems from a local data centre to a cloud environment can impact performance in core banking operations.
Reason (R): The physical distance between the data centre and data entry point can introduce latency issues.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2021**

**121.** Read the following case study and answer the questions that follow.
*A bank's foreign exchange desk requires a system that provides information on securities and money markets. Dealers make payments through the bank, and accounting entries must be created instantly to keep the organization's book up to date. Delays of even seconds can result in massive financial losses.*
Due to the highly dynamic nature of the inputs from the dealers, if the system fails, it would be difficult to audit or recover. How does the system primarily handle this risk?
(A) By restricting dealer input to fixed time intervals only.
(B) By reverting to analogue computing methods.
(C) By running parallel batch processing alongside real-time operations.
(D) By providing system checkpoints for every two to three minutes.

**Oct/Nov 2019**

**122.** Read the following case study and answer the questions that follow.
*The Clearing Department of a Central Bank handles millions of physical cheques daily. Each cheque has account details printed using special ink. The cheques are fed into a machine, read, sorted by settlement bank, and processed in one massive uninterrupted run to determine the net settlement amount.*
During the cheque processing run, the day's collected cheques form a file that updates the bank's main ledger. In data processing terminology, the file formed by the day's collected cheques is called the:
(A) Master file
(B) Error file
(C) Transaction file
(D) Encrypted file

**May/June 2017**

**123.** Read the following case study and answer the questions that follow.
*Bank Sigma's Risk Analytics division needs to run*

Downloaded from www.pdf.tube

*a complex scientific risk-modeling algorithm that requires massive computational power. Instead of buying a supercomputer, the IT team writes software that farms out small pieces of the mathematical problem to the unused processor cycles of 10,000 employee PCs during their idle time.*

The software utilized by Bank Sigma to manage and allocate the processing tasks across the 10,000 PCs is functionally similar to which of the following tools?

(A) Microsoft Hyper-V
(B) Oracle Cloud
(C) Sun's Grid Engine, a distributed resource management tool.
(D) Salesforce CRM

**Oct/Nov 2015**

**124.** Read the following case study and answer the questions that follow.

*A bank's foreign exchange desk requires a system that provides information on securities and money markets. Dealers make payments through the bank, and accounting entries must be created instantly to keep the organization's book up to date. Delays of even seconds can result in massive financial losses.*

The system supporting the forex dealers is best described as a:

(A) Dealer support system functioning as a high-speed real-time system.
(B) Centralized batch processing system
(C) Desktop virtualized network
(D) Storage area network (VSAN)

**May/June 2023**

**125.** Read the following case study and answer the questions that follow.

*Bank Sigma's Risk Analytics division needs to run a complex scientific risk-modeling algorithm that requires massive computational power. Instead of buying a supercomputer, the IT team writes software that farms out small pieces of the mathematical problem to the unused processor cycles of 10,000 employee PCs during their idle time.*

This approach used by Bank Sigma is formally known as:

(A) Desktop Virtualization
(B) Grid Computing
(C) SaaS Cloud Computing
(D) Local Area Clustering

NODIA

# ANSWERS

1. (D) John Von Neumann
In 1946, John Von Neumann introduced the stored program concept, a revolutionary idea in early computing. This design allowed both data and programmed instructions to be stored within the same internal memory of the computer. Previously, machines required physical rewiring for different tasks, but this concept enabled greater flexibility and paved the way for modern electronic computer architecture.

2. (C) The number of virtual servers that can run on a single physical host machine.
The consolidation ratio in server virtualization identifies how many virtual server instances can operate efficiently on a single physical hardware host. A higher ratio indicates better resource utilization, as multiple isolated operating systems share the host's processing power and memory. This metric is essential for organizations aiming to reduce physical server sprawl, energy costs, and data center space requirements.

3. (C) A network sharing many computers' resources simultaneously to solve a single problem.
Grid computing involves a distributed architecture that links numerous networked computers to function as a large virtual supercomputer. This model allows for the simultaneous sharing of diverse resources, such as processing power and storage, across different geographic locations to tackle complex computational problems. Unlike centralized systems, it utilizes decentralized resources efficiently to handle massive data processing tasks or scientific simulations.

4. (C) An application must traverse two operating systems, increasing processing time and overhead.
Hardware virtualization imposes performance limitations because an application running within a virtual machine must communicate through both the guest operating system and the host hypervisor. This additional layer of abstraction consumes extra processing cycles and memory resources, leading to increased latency. Consequently, while virtualization offers flexibility, it inherently introduces overhead compared to running an application directly on a physical server.

5. (B) A master file holds permanent records, while a transaction file stores periodic updates.
In computerized data processing, files are categorized based on their stability and usage. A master file functions as a long-term storage unit for permanent records, such as employee names or bank account balances. In contrast, a transaction file is temporary and captures specific events or changes, which are later used to update the master file during a scheduled processing run.

6. (B) They measure continuous physical magnitudes and provide approximate results.
Analogue computers represent data through continuous physical variables, such as voltage, pressure, or temperature, rather than discrete digits. These machines perform calculations by measuring changes in these magnitudes, making them highly effective for scientific and engineering simulations where precision is balanced with speed. Because they deal with varying physical states, the results provided are typically approximations reflecting the measured inputs.

7. (B) A finite sequence of instructions followed to solve a problem or process data.
An algorithm is a precise, step-by-step set of instructions designed to perform a specific task or solve a computational problem. In the context of computer processing, algorithms define the logic that transforms raw input data into meaningful output. For an algorithm to be effective, it must consist of a finite number of well-defined steps that eventually lead to a conclusion.

8. (B) Real-time systems exercise control during operation where delays cause critical failure.
Real-time systems are distinguished by their need to process data and provide immediate responses within strict time constraints. These systems exercise direct control over ongoing processes,

Click Here to Buy book on Amazon

where any delay beyond a specific threshold could lead to system failure or catastrophic results. Unlike standard on-line systems that manage interactive transactions, real-time environments must ensure deterministic timing to maintain operational safety and accuracy.

**9.** (B) It applies the resources of multiple networked computers to solve one problem at once.
Grid computing functions by aggregating the processing power and storage capacity of many geographically dispersed computers to work on a single, large-scale task. This collaborative approach enables the system to perform complex calculations that would exceed the capability of an individual machine. Specialized software is required to partition the workload and manage the various networked resources effectively across the entire grid.

**10.** (C) 50000 transistors
Fourth-generation computers marked a significant advancement in technology with the introduction of Very Large Scale Integrated (VLSI) circuits. These chips consolidated thousands of individual components, such as transistors, onto a single silicon wafer. Specifically, a standard VLSI chip during this era was capable of holding approximately 50,000 transistors, facilitating the creation of powerful microprocessors and the eventual rise of personal computers.

**11.** (D) It separates the user's physical device from the OS, storing data on a remote server.
Desktop virtualization is a technology that uncouples the operating system and applications from the physical client device used by the individual. Instead of running locally, the desktop environment is hosted and managed on a remote central server. This allows users to access their personal workspace from any compatible device, while data remains securely stored and processed within the data center infrastructure.

**12.** (C) A computer combining the features and capabilities of digital and analogue machines.
A hybrid computer integrates the high precision of digital systems with the rapid processing of continuous signals characteristic of analogue machines. These specialized systems are designed to convert analogue inputs into digital data for complex logical operations. They are frequently utilized in advanced simulations, such as guiding missile systems or monitoring complicated industrial processes, where both continuous measurement and discrete calculation are necessary.

**13.** (A) Customers pay for computing resources based on usage, similar to electricity billing.
The utility computing model transforms IT resources into a metered service, where users are charged based on their actual consumption of processing power, storage, and bandwidth. This approach mirrors public utilities like electricity or water, allowing organizations to avoid significant upfront capital expenditures. By adopting this model, cloud service providers enable businesses to scale their infrastructure dynamically while only paying for what is used.

**14.** (C) Because scientific tasks involve low I/O volume but require complex computations.
Scientific applications prioritize high computational speed because they often involve intricate mathematical models and simulations that require intense processor activity. Unlike business applications that handle massive amounts of input and output data, scientific tasks generally process smaller volumes of information but perform millions of complex calculations. Therefore, the ability of the CPU to execute these operations rapidly is crucial for achieving timely results in scientific research.

NODIA

**15.** (D) In the second generation, magnetic core storage was used to build large RAM systems.
Second-generation computers moved away from the bulky vacuum tubes of the previous era, adopting transistors for switching and magnetic core storage for primary memory. Magnetic core technology allowed for the development of significantly larger and more reliable random-access memory systems. This advancement in memory architecture was essential for supporting more complex programs and improving the overall processing efficiency of computers during that period.

**16.** (A) The systematic capture, storage, and transformation of facts into useful information.
In business administration, data processing is defined as the organized method of gathering raw facts and converting them into meaningful

information. This process involves capturing transactions, storing records securely, and applying logic to analyze the data. The ultimate goal is to provide decision-makers with accurate insights that support organizational activities, such as financial reporting, inventory management, and strategic planning for the future.

**17.** (A) It provides a full software application hosted on the cloud via a pay-per-use model.
Software as a Service is a cloud delivery model where a third-party provider hosts applications and makes them available to customers over the internet. Users typically subscribe to these services on a pay-per-use basis, eliminating the need to install or maintain software on local hardware. Examples include customer relationship management tools and web-based email, which offer scalability and reduced management overhead.

**18.** (A) 2800 milliseconds
Charles Babbage's Analytical Engine, designed in the 19th century, was an ambitious mechanical computer intended to perform complex calculations automatically. According to Babbage's technical specifications, the machine was estimated to take approximately 2800 milliseconds to multiply two numbers. While extremely slow by modern standards, this design laid the conceptual foundation for programmable computing and the mechanical execution of arithmetic operations through a series of gears.

**19.** (D) Reducing energy usage and hazardous waste by replacing physical servers with virtual ones.
Green computing focuses on minimizing the environmental impact of information technology through energy efficiency and sustainable practices. A primary strategy involves utilizing virtualization to consolidate multiple virtual servers onto fewer physical machines, thereby significantly reducing power consumption and electronic waste. This approach helps organizations decrease their carbon footprint while lowering operational costs associated with cooling and maintaining large-scale physical data center infrastructures.

**20.** (A) It prevents simultaneous updates by locking a record while it is being modified.
Record locking is a critical concurrency control mechanism used in on-line transaction processing systems. When a user accesses a specific record for modification, the system prevents other users from making changes to that same record until the first transaction is finalized. This ensures data integrity by preventing conflicting updates, which could otherwise lead to inaccurate information and inconsistencies within the database.

**21.** (C) A modular, stripped-down server designed to minimize physical space and energy usage.
A blade server is a specialized hardware architecture where multiple thin, modular server cards are housed within a single chassis. By stripping away redundant components such as power supplies and cooling fans, these servers optimize physical space and reduce energy consumption in data centers. This high-density design allows for easier management and scalability, making it an efficient choice for large-scale enterprise computing environments.

**22.** (B) 60 additions a minute
The Analytical Engine, conceptualized by Charles Babbage in 1837, was a pioneering mechanical design for a general-purpose computer. It was intended to perform mathematical operations using a series of interlocking gears and wheels. For basic arithmetic, the engine was planned to operate at a computational speed of sixty additions per minute. This benchmark represented a significant advancement in the vision of automated data processing.

**23.** (D) Data refers to raw meaningless facts, while information conveys meaning based on facts.
Data consists of raw, unprocessed facts, figures, or observations that lack context and meaning on their own. In contrast, information is produced when data is organized, analyzed, and presented in a way that provides value to the user. While data serves as the essential input for processing, information is the meaningful output that facilitates decision-making and understanding within a specific context.

Downloaded from www.pdf.tube

**24.** (D) It combines private clouds for sensitive data with public clouds for standard workloads.
A hybrid cloud is a strategic computing environment that integrates private and public cloud infrastructures. This model allows organizations to maintain sensitive data and critical applications within a secure private cloud while utilizing the scalability and cost-effectiveness of a public cloud for less sensitive workloads. By bridging these two environments, businesses achieve greater flexibility, improved resource optimization, and better compliance with security regulations.

**25.** (B) Linking computers and devices to appear to external users as a single available system.
Cluster computing achieves high availability by connecting multiple independent computers to work together as a single unified system. From the perspective of an external user, the cluster appears as one powerful resource. This architecture ensures that if one machine fails, others in the cluster can take over its tasks seamlessly. This redundancy is vital for mission-critical applications requiring five-nines of operational uptime.

**26.** (D) The physical components of which a computer is made up.
In a computerized environment, hardware encompasses all the tangible, physical parts of the computer system. This includes internal components like the central processing unit, memory modules, and circuit boards, as well as external peripheral devices such as monitors, keyboards, and storage drives. Hardware provides the physical infrastructure necessary to execute software instructions and process data, forming the foundation of any computing machine.

**27.** (A) Communication costs are reduced as most processing occurs on local on-site computers.
Distributed data processing involves a network of geographically dispersed computers that handle tasks locally rather than relying on a single central mainframe. By performing most computations at the site where data is generated, organizations can significantly reduce the volume of information transmitted over long distances. This localized approach leads to lower communication costs and improved system performance, as bandwidth requirements are effectively minimized.

**28.** (A) Every two to three minutes
Real-time systems are highly dynamic, with files and records changing constantly due to continuous input. To ensure that these systems can be recovered or audited effectively after a failure, checkpoints are established at frequent intervals. Typically, these checkpoints occur every two to three minutes, capturing the system's state and transaction history. This frequent logging minimizes data loss and facilitates a rapid return to operation.

**29.** (C) Germanium transistors were replaced by Silicon transistors and Integrated Circuits.
Third-generation computers introduced significant technological breakthroughs by replacing individual germanium transistors with integrated circuits made of silicon. These circuits allowed thousands of components, such as transistors and resistors, to be packed onto a single small chip. This advancement dramatically increased processing speed and reliability while reducing the physical size and power consumption of the machines, moving away from discrete hardware components.

**30.** (D) To restore a file to its state before an update or re-apply changes after a failure.
In on-line processing, rollback and roll forward are essential recovery procedures. Rollback allows the system to undo incomplete or erroneous updates, returning a file to its original state before a specific transaction began. Conversely, roll forward uses transaction logs to re-apply successful updates to a backup copy of the master file after a system crash. Together, these processes maintain data consistency and integrity.

**31.** (C) The duplicate OS consumes disk space but does not need to be licensed separately.
A significant limitation of hardware virtualization is the impact on resource consumption and compliance. Each virtual machine requires its own guest operating system, which consumes valuable disk space and memory on the physical host. Furthermore, these instances typically require separate software licenses, increasing operational costs for the organization. Ignoring these requirements can lead to both performance bottlenecks and legal risks related to software usage.

NODIA

**32.** (B) Total elimination of the need for operating systems
Server virtualization offers numerous advantages, including reduced electrical consumption, decreased floor space requirements, and improved organizational profitability through better resource utilization. However, it does not eliminate the need for operating systems. Instead, virtualization relies on multiple operating systems running simultaneously as virtual machines on a single physical host. Each virtual instance still requires its own operating system to manage applications and interact with the hypervisor.

**33.** (B) The transaction file must always be sorted in the same order as the master file before updating.
On-line transaction processing is characterized by the immediate updating of master files as transactions occur. Unlike batch processing, which requires transaction records to be grouped and sorted in the same sequence as the master file, OLTP systems process individual events randomly and instantly. This allows for real-time validation and data storage on secondary devices, ensuring that the system always reflects the most current information available.

**34.** (D) The failure of the main computer causes all remote terminals to suspend operations.
In a centralized timesharing system, multiple remote terminals rely entirely on a single powerful central processor. While this model allows for efficient sharing of resources, it creates a significant single point of failure. If the main computer crashes, all connected terminals lose access and must stop their operations immediately. This lack of redundancy makes the entire organization vulnerable to downtime whenever the central system experiences technical issues.

**35.** (A) Integration of artificial intelligence and natural language processing techniques.
Second-generation computers were defined by the transition from vacuum tubes to transistors, resulting in machines that were smaller, more reliable, and consumed less power. These computers were much more efficient at dissipating heat and required less physical space. However, advanced concepts like artificial intelligence and natural language processing were not characteristic of this era; these features are defining elements of the fifth generation of computer development.

**36.** (A) They use intelligent programming and artificial intelligence to interpret natural languages.
Fifth-generation computers represent the ongoing effort to create machines capable of human-like reasoning. These systems utilize artificial intelligence and advanced programming techniques to understand and process natural language input. By moving beyond traditional binary logic, they aim to interact with users more intuitively. This generation focuses on parallel processing and highly sophisticated software to achieve intelligence that mimics human thought and complex problem-solving abilities.

**37.** (A) The CONTROL UNIT converted continuous physical magnitudes into numerical indications.
Charles Babbage's Analytical Engine consisted of several key components inspired by industrial textile mills. The store held numbers and intermediate results, while the mill functioned as the arithmetic unit, performing calculations through gear rotations. An input device entered instructions via punch cards. However, the control unit did not convert continuous physical magnitudes; instead, its primary role was to manage the correct sequence of operations within the mechanical system.

**38.** (D) Magnetic Ink Character Recognition (MICR) reader/sorter
On-line enquiry systems allow users to retrieve specific information from databases quickly using tools like Structured Query Language or fourth-generation languages. Macros are often employed to automate repetitive query tasks. In contrast, Magnetic Ink Character Recognition readers are physical hardware devices used in batch processing environments, specifically for sorting and reading pre-printed data on cheques. They are not used for interactive on-line queries or data analysis.

**39.** (D) These routines occur after business hours and do not require high-cost online processing.
Banking systems utilize batch processing for tasks like interest calculations because these routines involve large volumes of data that do not

Click Here to Buy book on Amazon

require immediate results. Since these operations typically occur after business hours when customer activity is low, they can be processed sequentially in one run. This approach is more cost-effective than using expensive real-time resources for non-urgent administrative tasks that are perfectly suited for overnight execution.

**40.** (D) Google App Engine serves as an IaaS requiring high initial fees for data storage.
The cloud computing landscape includes several major service models and providers. Amazon Web Services offers infrastructure via EC2, while Salesforce is a prominent SaaS provider for customer relationship management. Microsoft provides web-based productivity tools like Exchange Online. However, Google App Engine is primarily classified as a Platform as a Service, offering a development environment rather than acting as a traditional Infrastructure as a Service with high initial storage fees.

**41.** (B) II, III, V, I, IV
The evolution of computer hardware began with vacuum tubes in the first generation. These were followed by germanium and silicon transistors in the second generation. The third generation introduced Integrated Circuits, while the fourth generation was defined by microprocessors using Very Large Scale Integration. Finally, the fifth generation and modern computing utilize Ultra Large Scale Integrated chips, representing a clear chronological progression of miniaturization and increased processing power.

**42.** (C) It requires companies to expand procurement processes and duplicate administrative skills.
Cloud computing provides numerous benefits, such as improved resource utilization, rapid scalability, and cost-effective redundancy. It allows organizations to focus on core business activities by outsourcing infrastructure management to specialized vendors. Far from requiring an expansion of complex procurement or duplication of skills, the cloud model simplifies IT administration by delivering resources on-demand and reducing the need for extensive in-house hardware acquisition and management.

**43.** (B) Amazon Elastic Compute Cloud (EC2)
Software as a Service refers to applications delivered entirely over the internet, such as Gmail, Hotmail, and Salesforce CRM. These tools allow users to access software without managing underlying infrastructure. In contrast, Amazon EC2 is an example of Infrastructure as a Service. It provides virtual servers and raw computing power upon which users can install their own operating systems and applications, rather than being a finished software product.

NODIA

**44.** (D) Germanium transistors
Fourth-generation computers are characterized by the development of microprocessors using Very Large Scale Integration technology, which enabled the creation of powerful personal computers and graphical user interfaces. These advancements allowed for decentralized computing and the growth of networks. However, germanium transistors are associated with the second generation of computers; by the fourth generation, silicon-based microchips had long replaced individual transistors as the primary building blocks.

**45.** (C) It improves utilization rates, reduces costs, and increases application development speed.
In the utility computing model, sharing intangible computing resources among multiple tenants allows for more efficient use of hardware. This pooling of resources ensures that idle capacity is minimized, leading to improved overall utilization rates. As a result, organizations can benefit from lower costs through economies of scale and faster application development, as infrastructure can be provisioned rapidly without the delays associated with physical hardware acquisition.

**46.** (B) Transaction data is fed into storage under CPU control without requiring prior sorting.
Batch processing is designed for the effective handling of large volumes of similar transactions grouped together. A key requirement of this method is that transaction items must be sorted in the same sequence as the records in the master file before the update process begins. This ensures that the master file can be updated sequentially and efficiently in a single, uninterrupted run, which is the hallmark of batch systems.

47. (B) A tool allowing engineers to pool computer cycles across workstations for management.
Sun Microsystems developed Grid Engine as a specialized software tool designed for distributed resource management. It enables organizations to aggregate the unused processing cycles of numerous networked workstations into a single pool of computing power. This allow engineers and researchers to run large-scale computational tasks across the network, optimizing the use of existing hardware and facilitating the management of complex workloads within a grid computing environment.

48. (B) In all grid architectures, computers must be managed by a single central mainframe system.
Grid computing utilizes a decentralized approach where multiple networked computers collaborate to solve complex problems. While it requires software to divide and distribute tasks, it does not depend on a central mainframe for management. Grid architectures can be deployed within a single corporation or across the public domain, as seen in projects like SETI@home, which harnesses idle processor cycles from millions of individual PCs globally via the internet.

49. (A) Apple
The virtualization market features several major technology providers that compete with VMware. Companies such as Citrix, IBM, and HP offer various software and hardware solutions to facilitate server consolidation and resource management. These organizations provide the infrastructure and platforms necessary for enterprises to implement virtualization strategies. Apple, while a prominent technology company, is not traditionally considered a primary provider of enterprise-level server virtualization systems like the others mentioned.

50. (C) Transaction items are stored on secondary storage under CPU control without prior sorting.
Batch systems follow a structured sequence where documents are sorted by type and assigned headers with control totals. A fundamental step in this process is sorting the transaction file to match the order of the master file. Only then can the system sequentially process the items to create a new, updated version of the master file. This ordered approach is necessary for efficient data processing and maintaining accurate historical records.

51. (D) To promote and recognize energy-efficiency in monitors and consumer electronics.
The ENERGY STAR program was established by the U.S. Environmental Protection Agency in 1992 as a voluntary labeling initiative. Its primary goal is to identify and promote energy-efficient products, such as computer monitors and other consumer electronics, to reduce greenhouse gas emissions. By setting performance standards, the program encourages manufacturers to develop hardware that consumes less power, thereby contributing to broader environmental sustainability goals within the technology industry.

52. (D) Physical distance between a data centre and a data entry point has no impact on performance.
Cloud computing faces several challenges, including the difficulty of budgeting on-demand costs and the high price of bandwidth for data-intensive tasks. Security is also a concern, as hacking can lead to collateral damage across multiple clients. Crucially, the physical distance between the data center and the user significantly impacts performance by introducing latency, which can cause noticeable delays in sensitive operations such as core banking transactions.

53. (C) Millimeter Wave Unit
A modern electronic computer is built upon five fundamental functional units that work together to process data. These include the input unit for receiving data, the memory unit for storage, and the output unit for communicating results. Internal processing is managed by the arithmetic and logic unit, which performs calculations, and the control unit, which coordinates all system activities. A millimeter wave unit is not a standard component of this architecture.

54. (C) A setup where an organization uses private clouds for sensitive data and public clouds for scaling.
A hybrid cloud is a versatile deployment model where an organization utilizes a combination of private and public cloud environments. This configuration allows a company to store highly sensitive information on its own internal, secure infrastructure while leveraging the vast resources

NODIA

of a public cloud for less critical tasks or sudden bursts in demand. This approach provides a balance between security requirements and the need for cost-effective, rapid scalability.

**55.** (A) The inability to provision or de-provision servers dynamically based on demand.
Cloud computing is defined by its ability to provide on-demand resources, meaning the dynamic provisioning and de-provisioning of servers is a core feature, not a challenge. Actual challenges include security concerns such as collateral damage, the high cost of bandwidth for moving large data volumes, and latency issues that can hinder real-time operations like banking. These factors must be carefully managed when organizations transition their critical workloads to the cloud.

**56.** (A) They are static environments, making them very easy to audit and recover after a failure.
Real-time systems are characterized by their dynamic nature, as they must process random inputs at unpredictable intervals. Because the status of files changes continuously, these environments are actually quite difficult to audit and recover. To manage this complexity, checkpoints are frequently established, often every two to three minutes, to capture the system's state. These systems are essential where delays in exercising control could lead to disastrous operational outcomes.

**57.** (A) Increased fault tolerance, data protection, and redundancy provided at a lower cost.
Cloud computing enhances business continuity for financial institutions by offering high levels of redundancy and fault tolerance across multiple geographic locations. This infrastructure ensures that data is protected and services remain available even if a local failure occurs. By pooling resources, cloud providers can offer these robust security and backup capabilities at a significantly lower cost than what a single bank could achieve by building its own equivalent on-premise infrastructure.

**58.** (A) Cloud apps are accessible only via isolated LANs that are disconnected from the Internet.
Computing environments have evolved significantly over time. Fifth-generation computing focuses on natural language input, while the fourth generation introduced decentralization through networks and personal computers. Centralized processing utilizes a single mainframe serving multiple dumb terminals. However, cloud applications are fundamentally designed to be accessible over the internet rather than being restricted to isolated local area networks. The internet provides the necessary connectivity for users to reach cloud-hosted services from any location globally.

**59.** (C) A device performing arithmetical operations on numbers using rotations of gears.
In Charles Babbage's design for the Analytical Engine, the mill served as the arithmetic unit of the machine. It was engineered to perform basic mathematical operations, such as addition and multiplication, automatically through the mechanical rotation of multiple gears and wheels. This component represented the "processing" heart of the engine, analogous to the central processing unit in modern computers, by executing the calculations required for data processing tasks.

**60.** (B) They provide highly accurate results expressed in binary digits for financial billing.
Analogue computers are designed to handle data expressed as continuous physical magnitudes, such as voltage or temperature. Because they measure these variables rather than counting discrete units, their results are generally approximations. They are widely used for scientific and engineering simulations where varying quantities must be monitored. Unlike digital computers, analogue machines do not use binary digits to provide the precise numerical accuracy required for financial operations like billing and accounting.

**61.** (C) P-2, Q-4, R-1, S-3
Cloud service models are defined by the level of management they provide. Infrastructure as a Service offers hardware-related resources like storage and virtual servers. Platform as a Service provides a development environment for building applications. Software as a Service delivers complete applications, such as Salesforce, on a pay-per-use basis. Finally, Business Productivity Online Suite represents Microsoft's specialized cloud offering of its office productivity tools, illustrating a specific application of these models.

Downloaded from www.pdf.tube

**62.** (C) Both (I) and (II)
Cluster computing involves linking multiple independent computers to function as a unified system. This architecture provides high availability and load balancing, making it ideal for managing traffic on busy websites. To an external user, the entire cluster appears as a single, powerful computer rather than a collection of separate machines. By distributing the workload across various nodes, the system ensures consistent performance and reliability, effectively presenting a seamless interface to the world.

**63.** (A) P-2, Q-3, R-4, S-1
Computer generations are defined by their primary switching technologies. The first generation relied on vacuum tubes, while the second introduced transistors and magnetic core storage. The third generation saw Integrated Circuits replacing individual transistors, leading to smaller machines. The fourth generation was characterized by the microprocessor chip using Very Large Scale Integration, which enabled the development of personal computers. Each phase represented a massive leap in computing speed, reliability, and physical efficiency.

**64.** (B) (II) and (III) only
Cloud computing offers significant advantages by fostering innovation through easier access to IT resources without the need for physical hardware acquisition. It improves resource utilization by pooling capacity into large, efficient clouds that can be shared among many users. While it provides flexibility and rapid scalability, it does not force enterprises into rigid structures or increase downtime; instead, it typically enhances agility and reduces the time required to implement technological changes.

**65.** (A) Second Generation — Magnetic core storage and Transistors
The second generation of computers marked a transition from vacuum tubes to more reliable and compact germanium or silicon transistors. This era also saw the introduction of magnetic core storage as the primary form of memory, which offered greater capacity and speed than previous technologies. These developments were fundamental in reducing the physical size of computers while significantly increasing their processing capabilities and overall system efficiency compared to the first generation.

**66.** (A) (I), (II), and (III) only
Grid computing aggregates the resources of numerous computers to solve a single complex problem simultaneously. This model requires specialized software to partition the task into smaller pieces that can be farmed out to different machines. It is not restricted to public projects like SETI@home; a grid can also be confined within the network of a single corporation. Therefore, grid computing is defined by its distributed nature and resource-sharing capabilities across various networked environments.

**67.** (C) II, IV, I, III
Data processing has evolved through several distinct phases. It began with centralized mainframe computers using dumb terminals for access. This was followed by a decentralized phase where mini and micro-computers allowed tasks to be handled locally. The development of communication networks then led to distributed processing across various sites. Today, the field is dominated by grid and cloud computing, which offer highly efficient, on-demand resource sharing and massive parallel processing power.

**68.** (C) Both (I) and (II)
The history of computing is marked by pivotal conceptual breakthroughs. Charles Babbage's Analytical Engine was a landmark 19th-century design that envisioned a mechanical machine capable of performing sixty additions per minute. Later, in 1946, John Von Neumann introduced the stored program concept, which fundamentally changed computer architecture by allowing both instructions and data to be kept in memory. These two developments collectively provided the mechanical and logical foundations for modern electronic computing systems.

**69.** (B) (I) and (III) only
Special-purpose computers are designed with a fixed set of instructions dedicated to one specific task, ensuring high efficiency. In the business world, applications like credit card billing manage data for thousands of customers and require extensive storage capacity. Conversely, scientific applications usually have low input/output volumes but require extremely high

NODIA

computational speeds to handle complex math. Therefore, the requirements for business and scientific computing differ significantly based on data volume and processing complexity.

**70.** (C) P-2, Q-1, R-4, S-3
Virtualization encompasses several distinct technologies. Server virtualization allows multiple isolated operating systems to run on one physical host. Desktop virtualization separates the operating system from the physical client for remote access. A blade server is a modular, stripped-down hardware design optimized for space and energy. Lastly, Virtual Storage Area Networks virtualize storage resources to provide greater flexibility. Each of these concepts contributes to a more efficient and manageable modern information technology infrastructure.

**71.** (A) (I), (II), (III), and (IV)
Modern data processing utilizes various models depending on the task's urgency. Batch processing handles sorted transaction groups sequentially, often for non-urgent accounting routines like interest calculation. On-line transaction processing feeds data directly into storage for immediate updates. Tools like SQL and 4GL are then used to query this data effectively. These methods, combined with technologies like record locking, ensure that information remains accurate, consistent, and accessible across different operational requirements and timeframes.

**72.** (B) P-3, Q-1, R-4, S-2
Data processing methods are distinguished by their operational characteristics. Batch processing involves grouping and sorting transactions before sequential updates. In on-line transaction processing, data is fed directly into storage to update master records immediately. Real-time systems exercise control during functioning, requiring frequent checkpoints for safety. Distributed processing connects multiple computers over a network to share workloads. Each method is chosen based on the specific speed, reliability, and connectivity requirements of the business application.

**73.** (B) Only (II)
In an on-line transaction processing system, ensuring data integrity is paramount. This is achieved through record locking, a feature that prevents a record currently being updated by one user from being accessed or modified by another simultaneously. This mechanism prevents conflicting changes and maintains consistency. Furthermore, validation must occur before data is permanently written to the master file, ensuring that only accurate and authorized information is stored in the secondary storage units.

**74.** (C) Real-Time System — Front-office counter terminals and dealer support systems
Different data processing models serve specific organizational needs. Batch processing is ideal for non-urgent tasks like calculating interest after business hours, rather than airline reservations. Conversely, real-time systems are essential for front-office counter terminals and dealer support systems, where immediate responses are critical for operational success. OLTP is typically used for interactive transactions like ticket bookings, while centralized processing traditionally relies on a single mainframe rather than decentralized peer-to-peer resource sharing.

**75.** (B) (I), (III), and (IV) only
Distributed data processing facilitates rapid access to information across geographically dispersed locations. While it lowers communication costs by processing data locally, it introduces challenges regarding the confidentiality and integrity of programs and files. Users must also manage protocol conversions when connecting incompatible machines at different sites. This model enhances local autonomy and system resilience but requires careful oversight to maintain security and interoperability across the network of independent but interconnected computing resources.

**76.** (D) P-3, Q-4, R-1, S-2
The Analytical Engine's architecture featured distinct components for specific functions. The store was designed to hold numerical data and intermediate results. The mill functioned as the arithmetic unit, performing mathematical operations automatically. The control unit was responsible for verifying the correct sequence of operations, acting as the system's logic manager. Finally, the input device allowed for the entry of both numbers and instructions, completing the

Click Here to Buy book on Amazon

foundational design for an automated computing machine.

77. (D) (I), (II) and (III)
Real-time systems are inherently dynamic, as they must process random inputs at unpredictable intervals. Because the status of files changes continuously, providing checkpoints every two to three minutes is necessary for effective audit and recovery. These systems are commonly implemented in front-office environments, such as bank counter terminals, where immediate data processing and response are required to support customer service and dealer operations. This ensures that the system always reflects the most current state.

78. (D) P-2, Q-1, R-4, S-3
Major technology companies offer specialized cloud services. Amazon provides infrastructure through Elastic Compute Cloud, while Google offers the App Engine platform for developers. Microsoft delivers a range of services including Azure and Dynamics CRM Online. Sun Microsystems contributed through initiatives like Project Caroline and Network.com. Together, these providers illustrate the diverse range of infrastructure, platform, and software solutions available in the modern cloud computing market, each catering to different enterprise and development needs.

79. (B) Only (II)
Green computing aims to reduce the environmental impact of technology. A key initiative was the ENERGY STAR program launched by the U.S. Environmental Protection Agency to promote energy efficiency in electronic devices. While virtualization significantly reduces hardware costs and electrical consumption by consolidating servers, it does not increase power usage. By running multiple virtual instances on fewer physical machines, organizations decrease both their physical footprint and the energy required for cooling and operation in data centers.

80. (D) Check pointing — Grouping all daytime transactions for processing at midnight.
On-line transaction processing systems use specific mechanisms to ensure data integrity and recovery. Rollback restores a master file to its state before a failed update, while roll forward re-applies successful changes from a log. Record locking prevents simultaneous updates to the same record. However, check pointing is not about grouping transactions for delayed processing; rather, it involves frequently saving the system's state at short intervals to facilitate rapid recovery and audit after a failure.

81. (C) (I), (II), and (III) only
Hardware virtualization introduces several limitations, including increased processing overhead as applications must traverse two operating systems. Each virtual instance consumes critical memory and disk space, and typically requires separate software licenses. While virtualization offers benefits, it does not eliminate the risk of a single point of failure; if the host machine crashes, all hosted virtual servers are affected. Therefore, careful analysis of resource constraints and redundancy is essential before deploying a virtualized server environment.

NODIA

82. (A) P-2, Q-4, R-1, S-3
Cloud location models are defined by how infrastructure is shared. A public cloud is hosted by a vendor and shared among various organizations. An on-premise private cloud is dedicated strictly to one organization and hosted internally. Hybrid clouds combine internal deployments with external vendor services to balance security and scaling. Community clouds are shared by organizations with similar backgrounds, such as government entities. These models allow businesses to choose the best environment based on their specific needs.

83. (D) P-4, Q-1, R-3, S-2
Modern technology relies on several specialized tools and standards. Macros are sets of instructions used to automate repetitive tasks in queries. Protocols provide the essential rules for network communication in distributed systems. Magnetic Ink Character Recognition is a specialized reader technology used for sorting and processing physical cheques in batches. Finally, ENERGY STAR is a voluntary labeling program that promotes energy efficiency. Each of these elements serves a distinct role in improving processing efficiency, connectivity, and sustainability.

**84.** (D) (I), (II) and (III)
The cheque-clearing process in banks is a classic application of batch processing. Cheques feature account details printed in magnetic ink, which are read and sorted by specialized MICR machines. This allows cheques to be grouped by the settlement bank for efficient processing. Once details are exchanged, the final settlement is achieved by adjusting the accounts of the respective banks at the central bank. This structured system ensures the accurate and orderly movement of funds across the banking industry.

**85.** (D) Neither (I) nor (II)
In data processing, file types are defined by the nature of the information they store. A master file is permanent and contains stable records like employee names or tax codes. Conversely, a transaction file is temporary and captures periodic data, such as monthly hours worked, which is used to update the master file. Therefore, both definitions in the question are reversed; master files are for long-term records, while transaction files hold the data for specific, temporary updates.

**86.** (B) P-2, Q-3, R-4, S-1
Computers are classified based on their operation and purpose. Analogue computers measure continuous magnitudes, while digital computers process data as discrete digits for high accuracy. Hybrid computers combine features of both for complex simulations, such as guided missile systems. Special-purpose computers are engineered for one dedicated task, offering high efficiency but lacking the versatility of general-purpose machines. Each type is suited to specific applications, ranging from simple business processing to highly advanced scientific and military engineering tasks.

**87.** (B) (I), (III), and (IV) only
Cloud computing service models offer different level of support. IaaS provides foundational hardware like storage and servers, while SaaS delivers finished applications like Gmail and Salesforce. These services rely on large data centers with powerful infrastructure to host web services. However, Platform as a Service offerings from different vendors are typically not highly compatible; developers often face "vendor lock-in" because the tools and environments are proprietary. Understanding these distinctions is crucial for selecting the right cloud strategy.

**88.** (B) P-2, Q-3, R-4, S-1
Cloud computing presents several specific challenges. Latency refers to performance delays caused by the physical distance between data centers and users. Data residency involves compliance with government mandates regarding where information is stored. Collateral damage occurs when a security breach at one site impacts multiple clients sharing the same infrastructure. Finally, bandwidth cost represents the expense of moving large volumes of complex data over the network. Managing these factors is essential for ensuring reliable and secure cloud-based operations.

**89.** (A) (I) and (II) only
Computer generations are defined by specific technological leaps. The third generation introduced Integrated Circuits, which combined multiple components like transistors and resistors on a single chip. The fourth generation saw the arrival of microprocessors using Very Large Scale Integration, leading to powerful personal computers, networks, and graphical user interfaces. While the fifth generation focuses on natural language processing, it relies on artificial intelligence and advanced parallel processing rather than obsolete vacuum tubes, which belong to the first generation.

**90.** (A) IaaS — Offering a development platform strictly without virtual servers.
Cloud computing terminology is categorized into specific models. Infrastructure as a Service provides virtual servers and storage, while Platform as a Service offers a development environment for engineers to build applications. Software as a Service delivers complete applications to users on a pay-per-use basis. Deployment models like public and hybrid clouds describe how these resources are shared or integrated. Defining IaaS as a development platform without servers is incorrect, as servers are a core component of infrastructure offerings.

Downloaded from www.pdf.tube

**91.** (B) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
During the third generation, computer memory evolved as magnetic core storage was replaced by more efficient semiconductor memories. This transition was driven by the shift from germanium to silicon transistors, which enabled the creation of integrated circuits. These ICs allowed for many electronic components to be placed on a single chip, significantly increasing processing speed and memory density while reducing the physical size of the machine. Thus, silicon technology directly facilitated the advancement of semiconductor memory systems.

**92.** (C) Timesharing system
A timesharing system involves a single powerful central computer that allocates small slices of processing time to multiple users simultaneously. In the historical setup described, Bank Beta used this model where various "dumb terminals"—which have no independent processing power—were connected to a central mainframe. This allowed multiple branches to access the central resources, but it also meant that a failure of the main processor would cause all connected terminals to lose their ability to operate.

**93.** (C) (I), (II), (IV), and (V)
Virtualization provides significant benefits, including reduced hardware costs through server consolidation and improved manageability by centralizing resources. It offers a high return on investment by maximizing the consolidation ratio and leads to substantial savings in energy and floor space. However, it does not eliminate the need for software licenses. Each operating system instance running as a virtual machine typically requires its own separate license, which is an important operational cost that organizations must account for during deployment.

**94.** (C) Bank Gamma is billed for usage, avoiding capital expenditure on hardware.
The utility computing model allows organizations like Bank Gamma to treat IT infrastructure as a metered service. By using AWS, the bank can rent computing power on-demand and pay only for the resources it actually consumes. This eliminates the need for significant upfront capital investment in physical servers and allows the bank to avoid the costs of maintaining hardware for peak loads. This flexible billing model is a hallmark of modern cloud services and utility-based computing.

**95.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Some experts argue that private clouds do not fully embody the spirit of cloud computing because they lack the characteristic of multi-tenant resource sharing. In a private cloud, the infrastructure is dedicated solely to one organization, which contrasts with the public cloud model where resources are pooled across many different clients. Because the benefits of massive scale and shared costs are reduced in a dedicated environment, some view private clouds more as an evolution of traditional data centers.

**96.** (B) An application must traverse two OSs, equating to slower responses and overhead.
A critical limitation of server virtualization is the introduction of performance overhead. In a virtualized environment, each application must communicate through its own guest operating system as well as the underlying host hypervisor. This double layer of processing can lead to increased latency and slower response times compared to running on a physical machine. For a large organization like Bank Delta, this added overhead must be carefully balanced against the benefits of server consolidation and cost savings.

**97.** (D) All (I), (II), (III), (IV), and (V)
Every modern electronic computer performs five basic functions to process data effectively. The input unit receives raw facts, while the memory unit stores them for future use. The arithmetic-logic unit handles all mathematical calculations and comparisons. The control unit manages the execution of instructions to maintain system order. Finally, the output unit transforms processed data into meaningful information for the user. Together, these five components form the functional core of all computerized systems across different generations.

**98.** (A) Batch Processing
Batch processing is the most appropriate method for Bank Alpha's midnight routines, such as calculating interest and service charges. These

NODIA

tasks involve large volumes of data that can be grouped together and processed sequentially in one uninterrupted run. Since these operations occur after business hours when immediate response is not required, the bank can utilize its computing resources effectively and economically overnight, ensuring all accounts are updated by the start of the next business day.

**99.** (B) Hybrid Cloud
Bank Gamma is utilizing a hybrid cloud model by integrating two distinct deployment strategies. It maintains a private cloud for its highly sensitive core banking database to ensure security and regulatory compliance. Simultaneously, it uses a public cloud service from AWS to host its mobile applications and CRM software for better cost efficiency and scalability. By combining internal and external infrastructures, the bank achieves an optimal balance between protecting critical data and leveraging flexible cloud resources.

**100.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Real-time systems are notoriously difficult to audit and recover because they are highly dynamic. These systems must process random inputs at unpredictable intervals, which causes the status of files and records to change constantly. Unlike static batch systems, where states are clearly defined after each run, the continuous updates in real-time environments make it challenging to pinpoint the exact state at any given moment. Frequent checkpoints are therefore essential to mitigate these risks and facilitate system recovery.

**101.** (A) Batch Processing
The Clearing Department's method is a classic example of batch processing. In this scenario, millions of physical cheques are grouped together and sorted by settlement bank before being processed. The entire "batch" is then run through the system in one massive, uninterrupted sequence to determine final settlement amounts. This approach is highly efficient for handling large volumes of similar items where immediate individual updates are less important than the accurate completion of the total workload.

**102.** (A) (I), (III), (IV), and (V)
On-line enquiry systems provide immediate access to critical data, such as exchange rates and account balances, making them essential for financial organizations. These systems can display or print requested information and often operate against data that was updated earlier in batch mode. While they facilitate queries, they do not usually perform real-time transaction processing themselves. Furthermore, enquiries are built using advanced tools like SQL and 4GL, which are designed to make data retrieval more efficient and user-friendly.

**103.** (B) Record Locking
To prevent inaccuracies when multiple users attempt to update the same account simultaneously, a record locking feature is essential. This mechanism ensures that once a teller begins a transaction on a specific account record, the system "locks" it, preventing any other user from making changes until the first update is complete. This concurrency control is vital in banking to maintain data integrity and ensure that account balances accurately reflect all withdrawals and deposits without conflicting updates.

**104.** (D) Assertion (A) is false, but Reason (R) is true.
On-line processing systems absolutely require software security provisions and data integrity controls to prevent unauthorized access and conflicting updates. A key feature for maintaining consistency is record locking, which prevents multiple users from simultaneously modifying the same data entry. While the assertion that security is unnecessary is false, the description of record locking as a tool for ensuring data consistency is accurate. These features are critical for protecting sensitive information in any interactive, multi-user computing environment.

**105.** (C) Green Computing
By consolidating 800 servers into 60, Bank Delta is significantly reducing its physical hardware footprint and energy consumption. This practice directly supports the goals of green computing, which focuses on environmentally sustainable IT operations. Minimizing the number of physical machines leads to less heat generation and a reduction in hazardous electronic waste during disposal. These efforts help organizations

Click Here to Buy book on Amazon

lower their carbon footprint and contribute to broader environmental conservation while also improving operational efficiency and reducing data center costs.

**106.** (B) (I), (II), (IV), and (V)
Cloud computing involves several critical challenges that organizations must manage. These include security risks like collateral damage from shared infrastructure and latency issues that can delay time-sensitive banking operations. Data residency laws also impose limits on where information can be stored geographically. Additionally, the bandwidth costs for moving large amounts of complex data can be significant. While cloud providers offer service level agreements, these do not always fully guarantee flawless performance, making risk assessment essential for enterprises.

**107.** (A) SaaS
Utilizing Salesforce.com for Customer Relationship Management is a clear example of the Software as a Service model. In this arrangement, the software application is fully hosted and managed by the vendor in the cloud. Bank Gamma accesses the tool over the internet on a subscription or pay-per-use basis, without needing to install, maintain, or manage any of the underlying infrastructure or development platforms. This model allows the bank to deploy sophisticated software quickly and with minimal IT overhead.

**108.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Batch processing is unsuitable for time-sensitive tasks like railway reservations because it involves grouping transactions for later, sequential processing. This method does not provide the immediate updates required to ensure that seat availability is accurate in real-time. For reservation systems, where multiple users need instant feedback and immediate master file updates, on-line transaction processing is necessary. Therefore, the lack of timeliness in batch processing is the primary reason it cannot be used for high-speed, interactive booking applications.

**109.** (D) Distributed Data Processing
The new system implemented by Bank Beta is best defined as distributed data processing. In this architecture, individual branches use their own computers to handle local workloads while remaining connected via a communication network. This allows for resource sharing and better system resilience compared to a centralized mainframe. By processing data closer to where it is generated, the bank can reduce the frequency of long-distance data transmissions, lowering communication costs and preventing a single point of system failure.

**110.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Adopting virtualization with blade servers is an effective strategy for minimizing both physical space and energy consumption in data centers. Blade servers are modular, stripped-down computers that share common resources like power and cooling within a single chassis. By removing redundant components, these servers achieve a high-density design that is much more efficient than traditional rack-mounted hardware. When combined with virtualization, this allows organizations to run numerous server instances while occupying a significantly smaller physical and environmental footprint.

**111.** (D) MICR (Magnetic Ink Character Recognition)
Magnetic Ink Character Recognition is a specialized technology used primarily by the banking industry to facilitate the automated processing of cheques. This system uses ink containing iron oxide, which can be magnetized and read by specialized machines. These MICR readers can quickly and accurately interpret pre-printed account details and cheque numbers, even if they are obscured by stamps or handwriting. This technology is essential for the efficient sorting and grouping of cheques in large-scale batch processing environments.

**112.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Hybrid computers are engineered to combine the precision of digital systems with the continuous measurement capabilities of analogue machines. This integration is necessary for specialized

Downloaded from www.pdf.tube

applications, such as simulating guided missile systems, where both complex logical calculations and the processing of varying physical magnitudes are required. By leveraging the strengths of both computer types, hybrid systems can model complex real-world behaviors and industrial processes that would be difficult to represent using only digital or analogue technologies alone.

**113.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Grid computing is exceptionally effective for solving massive scientific or technical problems because it pools the resources of numerous networked computers. By applying the collective processing power of many machines to a single task at the same time, the grid can handle complex calculations that would exceed the capacity of an individual system. This collaborative architecture is designed to manage workloads that require a vast number of processing cycles, making it ideal for data-intensive research and large-scale simulations.

**114.** (B) Residency of data
The decision by Bank Gamma to host sensitive data internally is a direct response to data residency challenges. Residency refers to government-mandated regulations that dictate where certain types of information, especially financial and personal data, must be physically stored. By keeping its core banking database on its own infrastructure within specific legal jurisdictions, the bank ensures compliance with these regulatory standards. This approach mitigates the risk of violating laws that might prohibit storing sensitive customer information on foreign-hosted cloud servers.

**115.** (D) Front-office Real-Time System
When a bank teller provides an immediate account balance to a customer at the counter, they are utilizing a front-office real-time system. These systems are designed to process transactions and respond to enquiries instantly, ensuring that the information provided is current and accurate. Real-time processing is essential in this context because customer-facing operations require immediate data retrieval and updates to support service delivery. This contrasts with back-office batch systems, which typically process non-urgent data in scheduled groups after hours.

**116.** (D) (I), (II), (III), and (IV)
Computer generations are marked by significant technological milestones. The first generation used vacuum tubes, while the second introduced advanced languages like FORTRAN and COBOL. The third generation saw a tenfold increase in switching speed through Integrated Circuits. The fourth generation brought VLSI microprocessors, enabling modern personal computing. While the fifth generation focuses on natural language processing, it heavily utilizes artificial intelligence logic to mimic human reasoning, which contradicts the claim that it explicitly avoids such technology in its design.

**117.** (D) Virtualization of servers
The IT head is proposing server virtualization, a technology that allows multiple isolated operating systems to run simultaneously on a single physical server. By using software from providers like VMware, Bank Delta can consolidate its many individual physical machines into a much smaller number of high-capacity hosts. Each host runs several "virtual servers," which share the underlying hardware resources like CPU and memory. This consolidation significantly reduces hardware costs, power consumption, and maintenance requirements, leading to a more efficient data center.

**118.** (D) Assertion (A) is false, but Reason (R) is true.
Distributed data processing typically reduces communication costs rather than increasing them. This is because tasks are handled by local computers at various sites, minimizing the amount of data that must be transmitted over long distances to a central location. While the assertion that costs are significantly higher is false, the reason correctly identifies that local processing reduces the frequency and volume of data transmission. This decentralized approach improves performance and reduces bandwidth requirements, making it a cost-effective alternative to centralized mainframe systems.

**119.** (A) Maintaining program integrity while handling incompatible protocols.
In a distributed networked architecture, ensuring that different systems can communicate

NODIA

effectively is a major challenge. Bank Beta will need to manage protocol conversions if the machines used at various branches are incompatible with each other. Furthermore, maintaining the integrity and confidentiality of programs and data files becomes more complex in a decentralized environment. Users must be diligent in protecting these resources from unauthorized access or corruption while ensuring that software functions consistently across the entire distributed network.

**120.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Moving systems to the cloud can impact performance because the physical distance between the data center and the end-user introduces latency. This delay in data transmission can be particularly noticeable in core banking operations that require immediate response times, such as card authorizations. Since cloud resources are often located in geographically distant data centers, the time it takes for data to travel across the network can slow down interactive tasks, making physical proximity an important factor in system design.

**121.** (D) By providing system checkpoints for every two to three minutes.
To manage the risks inherent in highly dynamic real-time environments like a forex desk, systems use frequent checkpoints. These checkpoints are established every two to three minutes to capture the system's current state and transaction log. If a failure occurs, this frequent saving of data allows for a more accurate and efficient audit or recovery process. By minimizing the time between recorded states, the system ensures that any lost information can be reconstructed quickly, which is critical for preventing financial losses.

**122.** (C) Transaction file
In the context of cheque processing, the daily collection of cheques forms a transaction file. This file contains the temporary data captured during the day's events, such as account numbers and amounts. At a scheduled time, this transaction file is used to update the bank's main ledger, which serves as the master file. While the master file holds the permanent, long-term records of the bank, the transaction file captures the periodic changes and updates that must be applied to maintain accurate account balances.

**123.** (C) Sun's Grid Engine, a distributed resource management tool.
The software used by Bank Sigma to manage and distribute processing tasks is functionally equivalent to a grid engine. Tools like Sun's Grid Engine are designed to aggregate the unused computational cycles of networked workstations and allocate them to complex tasks. This distributed resource management allows organizations to harness their existing hardware to solve large-scale mathematical or scientific problems. By farming out small pieces of the workload, the system maximizes efficiency and provides supercomputing-like performance without the need for a dedicated high-cost supercomputer.

**124.** (A) Dealer support system functioning as a high-speed real-time system.
A system for a foreign exchange desk must operate as a high-speed real-time dealer support system. This is because dealers require instant access to market information and must create accounting entries immediately to keep records up to date. In the fast-paced money markets, even delays of a few seconds can lead to significant financial consequences. Therefore, the system must process random inputs instantly and exercise continuous control over transactions to ensure that the organization's books always reflect the most current financial position.

**125.** (B) Grid Computing
Bank Sigma is utilizing grid computing to solve its complex risk-modeling problem. This approach involves networking numerous individual computers and using specialized software to distribute pieces of a large task across their idle processor cycles. By pooling the collective power of 10,000 employee PCs, the bank creates a virtual supercomputer capable of handling massive computational workloads. This model is highly efficient for scientific or technical problems that require significant processing time, allowing the organization to achieve high-performance results using its existing infrastructure.

www.nodia.in

Click Here to Buy book on Amazon

# CHAPTER 03
# Introduction to Software

**Oct/Nov 2016**

**1.** What is the primary purpose of system software in relation to application programs?
(A) To provide highly advanced graphical elements and interface skins for user entertainment
(B) To translate complex natural language queries into structured relational database commands
(C) To replace the logical functions of a central processing unit during periods of heavy loads
(D) To insulate application programs from the complex operational details of the underlying hardware

**May/June 2022**

**2.** What makes the C programming language an elegant compromise for software development?
(A) It eliminates the need for any compilers by executing natively across all types of hardware.
(B) It restricts programmers strictly to machine-level memory manipulation without data structures.
(C) It bridges the gap between assembly language efficiency and high-level structural convenience.
(D) It is completely free from syntax requirements, allowing for flexible natural language inputs.

**Oct/Nov 2005**

**3.** What does a machine language, specific to an individual processor, consist of?
(A) Complex alphanumeric mnemonics representing sophisticated mathematical algorithms for general processing
(B) Syntactical blocks written in high-level code that human programmers can easily read and interpret
(C) Binary value groups representing processor instructions that change the computer state
(D) Permanent hardware-embedded codes that cannot be altered or executed within the system RAM

**May/June 2010**

**4.** How is application software defined?
(A) Software designed specifically to insulate various hardware variables from complex network operations
(B) The intrinsic code that operates hardware devices during the initial computer boot sequence
(C) Software that allows end users to accomplish one or more specific non-computer related tasks
(D) A suite of diagnostic tools intended for memory defragmentation and storage optimization

**Oct/Nov 2014**

**5.** Which of the following accurately describes the utilization of Linux as a server operating system?
(A) Linux is utilized by less than 10% of all cloud infrastructure providers.
(B) Linux is utilized by more than 95% of the top 1 million servers on the planet.
(C) Linux is primarily a desktop edition operating system with negligible server presence.
(D) Linux powers exactly 50% of all cloud infrastructure currently in use.

**May/June 2019**

**6.** Which of the following is a correct function of inventory management software?
(A) It manages internal computer hardware routing and system utility defragmentation.
(B) It tracks an organization's goods and materials on the basis of quality as well as quantity.
(C) It executes binary routines strictly to manage customer relationship operations.
(D) It provides functionalities solely for copying and retrieving corrupted backup data.

NODIA

**Oct/Nov 2021**

**7.** What is the general definition of computer software as described in the context of computer systems?
(A) The physical interconnections and specialized peripheral devices required for data storage and execution
(B) A set of programs, procedures, and documentation for performing tasks on a computer system
(C) The structural framework of high-performance microprocessors and their associated hardware components
(D) A specialized graphical utility designed exclusively for optimizing internal operating system execution

**May/June 2007**

**8.** Why is machine language considered the only language that can be understood by a computer without translation?
(A) It consists of alphanumeric characters and symbols that bypass the central processing unit.
(B) It uses binary patterns of ones and zeroes that digital processors execute as instructions.
(C) It utilizes physical hardware switches that directly connect to the computer motherboard.
(D) It is formulated in high-level mathematical expressions that are compiled instantaneously.

**Oct/Nov 2010**

**9.** Consider the following statements regarding Visual Basic and select the correct option:
I It is a cross between BASIC, Microsoft Office macro languages, and rapid application development tools.
II It was designed to prevent users from writing macros using Visual Basic for Applications (VBA).
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**May/June 2013**

**10.** Which mobile operating system holds the largest share of the mobile market?
(A) iOS
(B) Windows
(C) Android
(D) Symbian

**Oct/Nov 2024**

**11.** All of the following are characteristics of OEM software EXCEPT:
(A) It is sold in bulk to resellers.
(B) It is designed to be bundled with hardware.
(C) It typically excludes retail packaging, printed manuals, and installation instructions.
(D) It is legal to buy unbundled from its original hardware system.

**May/June 2016**

**12.** Practical computer systems divide software into three major classes. Which of the following is NOT one of these major classes?
(A) System software
(B) Programming software
(C) Middleware software
(D) Application software

**Oct/Nov 2018**

**13.** All of the following are examples of object-oriented third-generation programming languages EXCEPT:
(A) Fortran
(B) C++
(C) Ruby
(D) Java

**May/June 2023**

**14.** Consider the following programming languages developed during the creation of UNIX:
I C
II BCPL
III B
Which of the following represents the correct chronological order of their development?
(A) (II), (III), (I)
(B) (I), (II), (III)
(C) (III), (I), (II)
(D) (II), (I), (III)

**Oct/Nov 2009**

**15.** According to the stack of software in a computer model, which element sits directly immediately below the Systems Software layer?
(A) Applications Software
(B) Databases
(C) Spreadsheets
(D) Computer Hardware

Downloaded from www.pdf.tube

May/June 2011

**16.** How does software fundamentally interact with hardware at the lowest execution level within a computer system?
(A) Software is loaded into RAM and executed by the CPU through machine language instructions.
(B) Software is permanently loaded into the Read-Only Memory and executed by peripheral controllers directly.
(C) Software bypasses standard memory modules and modifies the hardware state via high-level language translation.
(D) Software functions completely independently of hardware by utilizing specialized, self-contained middleware engines.

Oct/Nov 2020

**17.** The following question consists of two statements — Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): In Fifth Generation Languages (5GL), the programmer only needs to worry about what problems need to be solved and the conditions to be met.
Reason (R): 5GLs are designed to make the computer solve a given problem without the programmer having to implement a routine or algorithm.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2005

**18.** Which of the following best defines an operating system?
(A) A program that organizes computer functions, manages jobs, and assigns them to proper locations
(B) A specialized hardware module that controls physical interconnects between the motherboard and devices
(C) A programming environment that merges compiling, interpreting, and debugging tools into one bundle
(D) A specific commercial application used exclusively to manage inventory and supply chain operations

Oct/Nov 2022

**19.** Which of the following pairs of a programming language and its defining characteristic is correctly matched?
(A) C# - A graphical macro language developed by Apple
(B) Perl - An object-oriented compiler strictly designed for 3D modeling
(C) Visual Basic - A complex assembly language used for supercomputers
(D) Java - Designed for portability utilizing a virtual environment

May/June 2018

**20.** What constitutes an Integrated Development Environment (IDE)?
(A) A software bundle merging text editors, compilers, and debuggers into a single interface
(B) A complex graphical interface designed for end-users to manage various mobile applications
(C) A dedicated hardware component that significantly accelerates local compiler execution speeds
(D) An independent third-party agent that holds the software source code in a legal escrow

NODIA

Oct/Nov 2017

**21.** Which of the following statements about utility software is incorrect?
(A) It is also known as a service routine.
(B) It helps in the management of computer hardware and application software.
(C) It performs a broad range of highly complex, organization-wide financial tasks.
(D) Disk defragmenters and virus scanners are typical examples of utility software.

May/June 2025

**22.** All of the following are included in the category of system software EXCEPT:
(A) Operating systems
(B) Word processors
(C) Device drivers
(D) Diagnostic tools

**Oct/Nov 2007**

**23.** Consider the following statements regarding Windows NT and select the correct option:

I Windows NT is an operating system that supports pre-emptive multitasking.

II There is only one version of Windows NT, which is designed exclusively to act as a server in networks.

(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**May/June 2014**

**24.** Consider the following statements about Fourth Generation Programming Languages (4GL):

I They are non-procedural languages that allow programmers to specify what the computer is supposed to do without specifying how.

II They generally require approximately ten times the number of statements compared to high-level languages to achieve the same results.

III They are generally used in conjunction with a database and its data dictionary.

Which of the above statement(s) is/are correct?
(A) (I) and (II)
(B) (II) and (III)
(C) (I) and (III)
(D) (I), (II), and (III)

**Oct/Nov 2025**

**25.** Which of the following statements about assembly languages is incorrect?
(A) They use mnemonic operation codes and symbolic addresses in place of 1s and 0s.
(B) They are highly portable and easily converted to run on any architecture without modification.
(C) They must be translated into machine language by a translator program called an assembler.
(D) They produce programs that are efficient, use less storage, and execute much faster than those from high-level languages.

**May/June 2009**

**26.** Which of the following statements correctly describes the translation of high-level programming languages?
(A) High-level languages are executed directly by the CPU without any intermediate translation.
(B) High-level languages must be assembled into object code using an assembler.
(C) High-level languages are mnemonic representations of natural language alphabets used exclusively for formatting.
(D) High-level languages are compiled or interpreted into machine language object code.

**Oct/Nov 2011**

**27.** Which of the following is cited as an example of general application software?
(A) MSOffice Suite
(B) Linux kernel
(C) BIOS updater
(D) Graphical User Interface (GUI) utility

**May/June 2021**

**28.** Consider the following events regarding the evolution of Microsoft Windows:

I Windows 7 overtook Windows XP as the most common version in use.

II Microsoft Windows was first released as an operating environment running on top of MS-DOS.

III Windows 95 was released, using MS-DOS as a bootstrap.

Which of the following represents the correct chronological sequence of these events?
(A) (I), (II), (III)
(B) (II), (III), (I)
(C) (III), (II), (I)
(D) (II), (I), (III)

**Oct/Nov 2006**

**29.** Which of the following pairs of a programming language and its feature is incorrectly matched?
(A) Python - Open-source, interpreted object-oriented language
(B) Ruby - Combines best features of several languages with clearer syntax
(C) COBOL - Primarily used for complex scientific and mathematical optimization
(D) Perl - Synonymous with CGI scripting and text processing

**May/June 2012**

**30.** Match the operating systems in List I with their corresponding descriptions in List II.
List I: (Operating Systems)

Click Here to Buy book on Amazon

P. HP-UX
Q. macOS
R. Solaris
S. Linux

List II: (Descriptions)

1. A hybrid kernel-based BSD variant
2. A free UNIX variant popular in academic environments
3. Descendant of System V Unix designed to run only on vendor's hardware
4. Can run on multiple types of hardware including x86 and Sparc servers

(A) P-3, Q-1, R-4, S-2
(B) P-1, Q-3, R-2, S-4
(C) P-4, Q-2, R-1, S-3
(D) P-3, Q-4, R-1, S-2

**Oct/Nov 2019**

**31.** ABC Bank procures a highly specialized core banking software from FinTech Solutions. The software is critical to the bank's daily operations. To mitigate the risk of FinTech Solutions going out of business or failing to provide support, ABC Bank insists on an agreement involving a neutral entity. The neutral entity will hold the software's source code and release it to ABC Bank only if specific triggers occur.
What is the precise term for this contractual framework?
(A) A Shared Source Initiative
(B) A General Public License Mandate
(C) A Software Escrow Arrangement
(D) An Open Standard Deposit

**May/June 2006**

**32.** Consider the following reasons individuals or organizations choose open source software:
I Lower cost
II Vendor lock-in guarantees
III Security
IV No vendor lock-in
V Better quality
Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (V)
(B) (I), (III), (IV), and (V)
(C) (II), (III), (IV), and (V)
(D) (I), (II), (IV), and (V)

**Oct/Nov 2023**

**33.** Consider the following categories:
I Adware
II System monitors
III Tracking cookies
IV Trojans
Which of the above are categories into which spyware is mostly classified?
(A) (I) and (II) only
(B) (II), (III), and (IV) only
(C) (I), (III), and (IV) only
(D) (I), (II), (III), and (IV)

**May/June 2008**

**34.** A startup company wants to enter the enterprise software market quickly. To reduce project costs and launch faster, they build their commercial software on top of existing robust open source platforms, utilizing external expertise.
This strategic move exploits which dimension of the open source model?
(A) Weaknesses
(B) Security threats
(C) Licensing threats
(D) Opportunities

**Oct/Nov 2012**

**35.** Which of the following statements about open source software licensing is incorrect?
(A) All open source software is universally covered by the GNU General Public License (GPL).
(B) Open source software may be licensed with terms allowing the work to be appropriated without making the new end product available to the public.
(C) The Open Source Initiative determines whether a license meets the requirements to be an "open source license."
(D) There are presently over 50 such licenses listed on the OSI web site.

**May/June 2024**

**36.** According to the Open Source Initiative (OSI), what is the core mandate for an 'open standard' regarding open source software?
(A) It must not prohibit conforming implementations in open source software.
(B) It must strictly mandate the use of the C++ programming language.
(C) It must prohibit the use of proprietary hardware in all deployments.
(D) It must require all developers to contribute financial royalties.

NODIA

Oct/Nov 2008

**37.** What is the fundamental operational premise of Shareware?
(A) It permits a free trial for a set period, after which it must be purchased or uninstalled.
(B) It remains permanently free for all commercial uses without any licensing or payment requirements.
(C) It requires constant internet bandwidth to upload new advertisements as part of the legal agreement.
(D) It disables only vital features like saving while allowing indefinite use of basic software functions.

May/June 2017

**38.** Consider the following statements and select the correct option:
I Python is an open-source programming and scripting language used to create web applications, mobile applications, and video games.
II PHP is a relational database management system (RDBMS) primarily utilized for creating 3D printed models and visual arts.
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

Oct/Nov 2013

**39.** Delta Corp decides to shift its infrastructure from proprietary platforms to an open source environment. The IT director emphasizes that the new system will allow the company to quickly deploy solutions, modify code as needed without paying seat license fees, and benefit from a rapid release rate for patches.
Which category of the open source SWOT analysis does this scenario best illustrate?
(A) Weaknesses
(B) Opportunities
(C) Threats
(D) Strengths

May/June 2020

**40.** Over five years, FinTech Solutions regularly updates the core banking software deployed at ABC Bank. According to the standard terms of their escrow agreement, how should the escrowed materials be managed regarding these updates?
(A) The escrowed code remains fixed at version 1.0 permanently to ensure total legal stability.
(B) ABC Bank must reverse-engineer the updates to supply the new source code to the agent.
(C) The escrow agent independently writes and inserts the updates into the stored code repository.
(D) The licensor is usually required to update the source code as the software package is upgraded.

Oct/Nov 2015

**41.** Which of the following statements regarding the 'Patents' requirement of an OSI open standard is incorrect?
(A) All patents essential to implementation must be licensed under royalty-free terms.
(B) The patents must allow for unrestricted use in conforming implementations.
(C) The patents can be covered by a promise of non-assertion when practiced by open source software.
(D) The patents must demand a standard royalty fee from all open source implementations.

May/June 2015

**42.** Under the GNU General Public License (GPL), consider the following specific "freedoms":
I The freedom to run the program for any purpose.
II The freedom to study how the program works and adapt it.
III The freedom to redistribute copies.
IV The freedom to improve the program and release improvements to the public.
V The freedom to patent the modified program for exclusive commercial monopoly.
Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (V)
(B) (I), (II), (III), and (IV)
(C) (II), (III), (IV), and (V)
(D) (I), (III), (IV), and (V)

Oct/Nov 2005

**43.** Consider the following statements regarding LibreOffice and VirtualBox:
I LibreOffice cannot preserve original Microsoft document formatting.
II LibreOffice includes a QR code generator tool for creating mobile-friendly links.

NODIA

III VirtualBox is a hosted hypervisor for x86 virtualization developed by Oracle Corporation.
IV VirtualBox allows users to run only one operating system at a time to maintain system stability.
Which of the above statement(s) is/are correct?
(A) (I) and (IV)
(B) (II) and (III)
(C) (I), (II), and (III)
(D) (II), (III), and (IV)

**May/June 2005**

**44.** A shared source arrangement typically does NOT permit which of the following actions?
(A) Limited sharing of proprietary source code with identified customer representatives
(B) Allowing individuals in enterprises to review code under protective conditions
(C) Reviewing the code by schools and governments
(D) Redistribution of the code or sharing with third parties

**Oct/Nov 2022**

**45.** Which of the following is cited as an example of an open standard in electronic commerce?
(A) The Python 3.0 object-oriented programming language.
(B) The Microsoft Windows NT internal system kernel.
(C) The Motion Picture Engineering Group compression standard (MPEG).
(D) The Universal Serial Bus (USB) physical hardware port.

**May/June 2011**

**46.** Match the types of software in List I with their appropriate descriptions in List II.
List I: (Software Type)
P. Crippleware
Q. Demo software
R. Adware
S. Spyware
List II: (Description)
1. Designed to demonstrate what a purchased version is capable of doing, acting like an automated tutorial
2. Transmits data covertly from a hard drive to obtain information about a user's activities
3. Supported by advertisements built into the program itself, requiring the user to view ads
4. Key features cease to work after the trial period ends, making the program largely unusable
(A) P-4, Q-1, R-3, S-2
(B) P-3, Q-2, R-1, S-4
(C) P-1, Q-4, R-2, S-3
(D) P-2, Q-3, R-4, S-1

**Oct/Nov 2020**

**47.** A government agency builds a custom portal relying heavily on a niche open-source project. Two years later, the core contributors abandon the project, leaving the agency with no 24/7 technical support and prone to increased schedule overruns for maintenance.
This scenario best aligns with which classification of open source characteristics?
(A) Global innovation opportunity
(B) Spiraling maintenance threats
(C) Customer involvement strength
(D) Extensible code strength

**May/June 2008**

**48.** Continuing from the previous scenario, the independent agent holding the source code for ABC Bank and FinTech Solutions operates under standard terms. If the agent successfully complies with its obligations of keeping the code secure and confidential, what is the agent's liability regarding the release and use of the source code and materials by ABC Bank?
(A) The agent bears full liability for any operational failures ABC Bank experiences.
(B) The agent has no liability in relation to the release and use of the source code.
(C) The agent assumes co-authorship liability if ABC Bank modifies the code.
(D) The agent is liable only for royalty-free patent assertions.

**Oct/Nov 2017**

**49.** The following question consists of two statements — Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): The advent of the modern Internet was a crucial driver for the growth of open source software.
Reason (R): The Internet serves as a mechanism for open source development communities to collaborate, which is necessary for successful

Downloaded from www.pdf.tube

development and improvements.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2016**

**50.** Match the open-source software in List I with its description in List II.
List I: (Software Name)
P. GIMP
Q. Mozilla Firefox
R. GNU
S. VLC
List II: (Description)
1. A web browser competing with Google Chrome, often default in Linux distributions
2. A multimedia application capable of playing audio and video files in any format
3. An image editing program that is a direct competitor to Adobe Photoshop
4. A congregation of software serving as a UNIX-like OS or part of an OS
(A) P-3, Q-1, R-4, S-2
(B) P-1, Q-2, R-3, S-4
(C) P-4, Q-3, R-1, S-2
(D) P-3, Q-4, R-2, S-1

**Oct/Nov 2025**

**51.** Which statement correctly describes the OSI's 'No Intentional Secrets' requirement for an open standard?
(A) The standard must withhold complex details to protect the creator's intellectual property.
(B) The standard must mandate the signing of a Non-Disclosure Agreement before implementation.
(C) The standard must depend exclusively on a patented, undisclosed hardware security algorithm.
(D) The standard must define a process for fixing flaws and incorporate changes into revised versions.

**May/June 2012**

**52.** The following question consists of two statements — Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): Under the GPL, the licensor allows the licensee to distribute copies of the covered software and charge for the service of distribution.
Reason (R): The GPL strictly equates the term "free" with "without cost," prohibiting any financial transaction related to the software distribution.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2010**

**53.** Which of the following statements correctly clarifies the relationship between commercial software and proprietary software?
(A) Commercial software is strictly synonymous with proprietary software in all legal instances.
(B) Proprietary software always provides users unrestricted access to inspect and modify the source code.
(C) Commercial software can be open source, so equating commercial with proprietary is incorrect.
(D) Commercial software cannot utilize proprietary source code due to Open Source Initiative guidelines.

**May/June 2018**

**54.** After implementing an open source CRM system, a mid-sized enterprise struggles because their internal staff cannot keep up with the rapid release rates of the software versions. Consequently, they are forced to hire external consultants whose fees are unexpectedly high.
This scenario exemplifies which aspect of open source software?
(A) Strengths
(B) Opportunities
(C) Weaknesses
(D) Cost efficiencies

NODIA

Oct/Nov 2024

**55.** Consider the following statements about various software:

I Blender is developed by an Amsterdam-based foundation for creating 3D graphics.

II MySQL is an important component of the LAMP stack used for data warehousing and e-commerce.

III Linux source code was originally created by Linus Trovalds in 1991 and is released under the GPLv2 licence.

Which of the above statement(s) is/are correct?

(A) (I) and (II)
(B) (II) and (III)
(C) (I) and (III)
(D) (I), (II), and (III)

May/June 2021

**56.** Which of the following correctly pairs the software classification with its legal modification status?

(A) Public domain software is the only type users can legally modify for their own purposes.
(B) Freeware can be legally modified by the end-user for his or her own purposes freely and easily.
(C) Public domain software always has a specific copyright owner who strictly prohibits modification.
(D) Shareware source code is made freely modifiable immediately after the thirty-day trial period.

Oct/Nov 2007

**57.** How are "open standards" defined?

(A) Public technical specifications developed via consensus without vendor limits.
(B) Proprietary guidelines developed by private firms for specialized internal use.
(C) Specific software licenses that enforce the GPL across all new hardware types.
(D) Legal documents required to initiate escrow arrangements with third-party firms.

May/June 2025

**58.** How is "source code" conceptually distinguished from "machine language" in the context of software execution?

(A) Source code is human-readable and must be translated into machine language for CPU execution.
(B) Source code consists strictly of ones and zeros, while machine language is readable by humans.
(C) Source code is executable directly by the CPU, whereas machine language requires a de-compiler.
(D) Source code is the native language of the computer, while machine language is the derivative work.

Oct/Nov 2018

**59.** The following question consists of two statements — Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.

Assertion (A): Proponents of open source software argue that it promotes more secure software compared to closed-source alternatives.

Reason (R): Source code transparency allows a wider group of people to inspect the software for flaws and vulnerabilities.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2007

**60.** In the typical open source software development model, what role does the "maintainer" play?

(A) A passive observer who only participates to monetize the final product for personal gain.
(B) An author or group that plays a key coordinating role in the software development project.
(C) An escrow agent responsible for securing the original source code from potential hackers.
(D) A legal entity that issues closed-source patents to various community members and developers.

Oct/Nov 2009

**61.** Regarding operating system compatibility, which two web browsers are explicitly noted to have compatible versions for all kinds of operating systems including Windows, macOS, Linux, BSD, Android, and iOS?

Click Here to Buy book on Amazon

(A) Internet Explorer and Edge
(B) Google Chrome and Safari
(C) Firefox and Opera
(D) Safari and Edge

**May/June 2014**

**62.** A multinational bank develops an interface strictly to allow its HR software to communicate with its payroll software on the company's private intranet. Outside users and internet-facing applications are completely blocked from accessing it.
This system is an example of a(n):
(A) Internal API
(B) Partner API
(C) Public API
(D) Open Standard API

**Oct/Nov 2014**

**63.** Match the open standards categories in List I with their corresponding examples in List II.
List I: (Category)
P. Hardware
Q. File formats
R. Protocols
S. Programing languages
List II: (Example)
1. HTML, XML, PDF
2. TCP, IP, SMTP, SNMP
3. PCI, USB
4. ANSI C, SQL
(A) P-1, Q-2, R-3, S-4
(B) P-3, Q-1, R-2, S-4
(C) P-3, Q-2, R-4, S-1
(D) P-2, Q-1, R-4, S-3

**May/June 2010**

**64.** Which of the following statements correctly identifies how a web browser handles unsupported file types?
(A) It permanently deletes the file from the remote server.
(B) It automatically decompiles the file into HTML.
(C) It forces the operating system to shut down to prevent malware execution.
(D) It prompts the user to save the file to disk rather than displaying it.

**Oct/Nov 2006**

**65.** Which of the following statements about PHP is correct?
(A) It is a scripting language primarily used for web development that can be embedded in HTML.
(B) It is primarily a 3D computer graphics software developed by an Amsterdam-based foundation.
(C) It is a hardware component known as the LAMP stack.
(D) It is an operating system created by Linus Trovalds in 1991.

**May/June 2013**

**66.** Why is the development of the Internet considered to have had a great deal to do with the growth of the open source development model?
(A) It provided a ubiquitous network for collaborative groups to host projects and maintain code versions.
(B) It allowed the central government to strictly regulate all international code writing activities.
(C) It forced all proprietary companies to legally surrender their patents to the public domain.
(D) It replaced the need for web browsers by allowing direct machine language file transfers.

**Oct/Nov 2011**

**67.** The 'No Agreements' criteria states there must NOT be any requirement for paperwork to deploy conforming implementations. Which of the following is an allowed requirement under the OSI criteria?
(A) Executing binding Non-Disclosure Agreements (NDA) prior to review.
(B) Accepting digital click-through agreements for legal indemnification.
(C) Compliance with royalty-free, freely available technical specifications.
(D) Obtaining signed license execution grants from the original authors.

**May/June 2017**

**68.** A customer inputs their credit card details on the frontend of an e-commerce application. The e-commerce store does not process the payment directly. Instead, it securely transmits the request to a payment processor, which creates a unique token for the transaction and returns it. This scenario perfectly illustrates the security

NODIA

benefit of which technological component?
(A) Open Source Hypervisors
(B) An Application Program Interface (API)
(C) A Fourth-Generation Natural Language Database
(D) An Open Standard Display Engine

**Oct/Nov 2019**

**69.** Which statement accurately describes the function of a layout/rendering engine in a web browser?
(A) It securely creates unique payment tokens for all electronic commerce transactions.
(B) It strictly filters out any JavaScript files to prevent malicious network assaults.
(C) It transforms HTML and associated content from mark-up into an interactive web document.
(D) It handles the mass distribution of OEM software to various hardware resellers.

**May/June 2009**

**70.** Which of the following statements about URL prefixes and browser handling is incorrect?
(A) The specific prefix used determines exactly how the following URL will be interpreted.
(B) The 'file:' prefix is used for accessing files stored on the user's local hardware.
(C) Prefixes the browser cannot handle are ignored and generate an error screen.
(D) 'news:' URIs are typically passed by the browser to the user's default newsgroup reader.

**Oct/Nov 2021**

**71.** What is the fundamental operational premise of a Fifth Generation Programming Language (5GL)?
(A) Solving a problem based on conditions without writing a routine or algorithm.
(B) Manually managing memory allocation through complex pointer arithmetic tasks.
(C) Translating assembly mnemonics into object code for embedded hardware systems.
(D) Designing specific user interfaces using object-oriented drag-and-drop tools.

**May/June 2023**

**72.** What is the definition of a web browser?
(A) A piece of specialized code that enables two distinct software programs to communicate directly.
(B) Software that lets users visit web pages on the Internet or access information on private networks.
(C) A hardware firewall appliance that filters HTML protocols for organizational security.
(D) A language translator that converts assembly codes into dynamic server-side scripts.

**Oct/Nov 2012**

**73.** An airline company provides a dedicated interface to a strategic hotel booking partner. The hotel's application must undergo a strict onboarding process and utilize specific login credentials to access the airline's flight schedule and pricing.
What type of API is being utilized in this arrangement?
(A) Open API
(B) Internal API
(C) Partner API
(D) Hardware API

**May/June 2024**

**74.** Which of the following conceptually best identifies the core definition of an API?
(A) An operating system kernel designed for mobile phones
(B) A graphical user interface utility for defragmenting disks
(C) A piece of code that enables two software programs to communicate
(D) A natural language processing tool for 5th generation programming

**Oct/Nov 2013**

**75.** Blender is utilized for all of the following applications EXCEPT:
(A) Creating 3D printed models
(B) Creating visual arts
(C) Giving the global community access to 3D technology
(D) Managing relational database data warehousing systems

**May/June 2006**

**76.** Which of the following best describes 'Wintel' in the context of open standards and architectures?
(A) A strictly proprietary closed hardware system with no public information sharing.
(B) A government-adopted telecommunications standard for high-speed fiber networks.
(C) A standard developed exclusively by the

Downloaded from www.pdf.tube

Internet Engineering Task Force (IETF).
(D) The widely accepted combination of Microsoft operating systems and Intel microprocessors.

**Oct/Nov 2008**

**77.** Which of the following statements regarding inventory management software is incorrect?
(A) It tracks goods and materials based on quality as well as quantity.
(B) It encompasses all internal warehouse movements and physical storage.
(C) It optimizes the flow of goods to improve general customer service.
(D) It is a required component of the OS kernel needed for system booting.

**May/June 2015**

**78.** Which of the following statements correctly identifies how a web browser handles unsupported file types?
(A) It permanently deletes the file from the remote server.
(B) It automatically decompiles the file into HTML.
(C) It forces the operating system to shut down to prevent malware execution.
(D) It prompts the user to save the file to disk rather than displaying it.

**Oct/Nov 2020**

**79.** Conceptually, how does an assembler fundamentally differ from high-level language compilers?
(A) Assemblers translate natural language into designs, while compilers execute code.
(B) Assemblers convert mnemonics to object code; compilers translate high-level code.
(C) Assemblers bypass object code for the GPU, while compilers rely on the main CPU.
(D) Assemblers create operating systems, while compilers create mobile applications.

**May/June 2019**

**80.** The following question consists of two statements — Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): APIs permit the abstraction of functionality, decoupling the consuming application from the service-providing infrastructure.
Reason (R): This abstraction entirely eliminates the need for any authorization credentials, allowing anonymous access globally without security vulnerabilities.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2015**

**81.** What is the primary limitation that prevents assembly languages from being universally adopted for all programming tasks?
(A) They produce highly inefficient programs that consume massive amounts of physical storage space.
(B) They are exclusively visual languages that lack syntax for complex mathematical optimization tasks.
(C) They are machine-dependent, require hardware knowledge, and are not easily portable to other computers.
(D) They do not require an assembler, leading to unverified and dangerous execution by the CPU.

**May/June 2020**

**82.** Based on the statistics available as of December 2021, what is the market share of Google Chrome?
(A) 19%
(B) 4%
(C) 65%
(D) 8%

**Oct/Nov 2016**

**83.** How did Microsoft fund the development costs for Internet Explorer?
(A) By selling it strictly as a standalone retail software package in physical computer stores.
(B) By forcing users to pay a monthly subscription fee for basic content rendering features.
(C) By running aggressive adware that constantly uploaded pop-up windows to user screens.
(D) By bundling it with Windows, effectively

NODIA

funding it via OS sales to manufacturers and users.

**May/June 2012**

**84.** The process known as "rendering" in a web browser involves transforming all of the following EXCEPT:
(A) HTML mark-up instructions.
(B) Server hardware RAM allocation.
(C) Associated image files.
(D) CSS formatting information.

**Oct/Nov 2022**

**85.** A weather forecasting service releases an interface allowing independent developers worldwide to freely pull basic weather data over the internet via HTTP without requiring any formal contracts or authentication.
Which specific type of API does this represent?
(A) Partner API
(B) Internal API
(C) Open (Public) API
(D) Escrow API

**May/June 2018**

**86.** Consider the following statements and select the correct option:
I "Open standards" are essentially the same entity as "open source software".
II There is no requirement that open standards must be implemented exclusively by open source software.
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**Oct/Nov 2023**

**87.** All of the following are characteristics or advantages of the Java programming language EXCEPT:
(A) It is designed specifically for high portability across different operating systems.
(B) It is much faster than applications written in compiled languages like C++.
(C) It utilizes a specialized "virtual environment" (JVM) to run programs effectively.
(D) It serves as a streamlined version of the C++ programming language for developers.

**May/June 2021**

**88.** Which of the following statements about web browser information resources and links is incorrect?
(A) Information resources may contain multiple hyperlinks to other relevant information resources.
(B) Each individual link contains the URI of a specific resource for the browser to locate.
(C) Clicking a link prompts the browser to navigate to the resource indicated by the target URI.
(D) Clicking a link forces the browser to restart the operating system to fetch the resource.

**Oct/Nov 2024**

**89.** From a fundamental perspective, what does software effectively do to the hardware of a computer?
(A) It permanently alters the physical semiconductor pathways on the motherboard during execution.
(B) It is a sequence of instructions for changing the state of computer hardware in a particular order.
(C) It replaces the need for random access memory by storing all instructions in logical loops.
(D) It restricts the central processing unit to a single binary state for the duration of its use.

**May/June 2022**

**90.** Consider the following steps involved when an API works:
I A client application makes an API call containing a request verb, headers, and sometimes a body via the API's URI.
II The API routes the physical network cables to the destination.
III The server responds to the API with the requested data, which is returned to the original application.
Which of the above statement(s) is/are correct?
(A) (I) and (II)
(B) (I) and (III)
(C) (II) and (III)
(D) (I), (II), and (III)

**Oct/Nov 2005**

**91.** Consider the following statements regarding Open Standards Requirement (OSR)

Click Here to Buy book on Amazon

Incompatible Dependencies and select the correct option:

I The standard must completely rely on closed-source technologies for security execution.

II Implementation of the standard must not require any other technology that fails to meet the criteria of this Open Standard Requirement.

(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**May/June 2010**

**92.** The following question consists of two statements — Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.

Assertion (A): API usage has exploded in the last decade, making many popular web applications impossible to create without them.

Reason (R): Developers do not need to understand the internal workings of an API; they only need to be able to communicate with other products and services using the interface.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2014**

**93.** Match the open source software in List I to its primary use in List II.

List I: (Open Source Software)

P. MySQL
Q. LibreOffice
R. VirtualBox
S. PHP

List II: (Primary Use)

1. Hosted hypervisor for x86 virtualization
2. Scripting language for web development managing dynamic content
3. RDBMS used for data warehousing and e-commerce
4. Includes programs for word processing, spreadsheets, and database management

(A) P-3, Q-4, R-1, S-2
(B) P-2, Q-1, R-4, S-3
(C) P-4, Q-3, R-2, S-1
(D) P-3, Q-2, R-1, S-4

**May/June 2011**

**94.** All of the following are characteristics of Adware EXCEPT:

(A) It is free software supported by advertisements built into the program.
(B) It sometimes requires a live Internet feed and uses constant bandwidth to upload new advertisements.
(C) It disables itself completely once the user's hard drive reaches full capacity.
(D) Disabling the ads is typically against the license agreement.

**Oct/Nov 2010**

**95.** Consider the following tools:

I Query languages
II Report generators
III Applications generators
IV Decision support systems

Which of the above tool(s) are categorized as fourth generation languages?

(A) (I) and (II) only
(B) (II) and (III) only
(C) (I), (II), and (III) only
(D) (I), (II), (III), and (IV)

**May/June 2005**

**96.** A freelance graphic designer downloads an advanced image editing tool for a 30-day trial. After 30 days, the program still opens and allows the designer to edit images, but the "save" and "export" functions are completely disabled, forcing the designer to purchase the license to finalize any work.

What classification of software does this describe?

(A) Public domain software
(B) Crippleware
(C) Open source software
(D) Adware

**Oct/Nov 2011**

**97.** Match the software categories in List I with their functions in List II.

List I: (Software Category)

P. Utility software
Q. Data backup and recovery software
R. Retail software

Downloaded from www.pdf.tube

S. Freeware

List II: (Function)

1. Provides functionalities beyond simple copying, allowing easy retrieval and original organization of files
2. Downloadable off the Internet free of charge, often for personal use only
3. Helps in managing computer hardware, performing small tasks like disk defragmentation
4. Sold off the shelves, generally more expensive, and comes with printed manuals

(A) P-3, Q-1, R-4, S-2
(B) P-1, Q-2, R-3, S-4
(C) P-4, Q-3, R-1, S-2
(D) P-3, Q-4, R-2, S-1

**May/June 2025**

**98.** The following question consists of two statements — Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.

Assertion (A): In very high-end systems like supercomputers, the share of the Windows OS is reduced to almost nil.

Reason (R): Unix and Unix-like operating systems are used in more than 99% of supercomputer systems due to their complexity and influential design.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2025**

**99.** Which statement correctly outlines the nature of public domain software?

(A) It requires a paid license for commercial use but is free for personal use.
(B) It is the only software users can legally modify for their own purposes.
(C) It is maintained by the Free Software Foundation under the GPL framework.
(D) It transmits data covertly to servers to profile internal user activities.

NODIA

**May/June 2007**

**100.** Consider the following statements regarding software licensing:

I Freeware does not contain spyware or adware.
II Demo software is fully functioning and intended for heavy commercial use indefinitely.
III Crippleware features a trial period after which vital features cease to work.

Which of the above statement(s) is/are correct?

(A) (I) and (II)
(B) (I) and (III)
(C) (II) and (III)
(D) (I), (II), and (III)

**Oct/Nov 2018**

**101.** A non-profit organization is migrating away from Microsoft Office 365 due to licensing costs. However, they possess thousands of legacy Microsoft files. They adopt an open-source alternative known to be superior due to its ability to better preserve Microsoft file formats, and it even includes a QR code generator for mobile-friendly links.

Which software did the non-profit organization adopt?

(A) LibreOffice
(B) Python
(C) GNU
(D) GIMP

**May/June 2013**

**102.** Match the open standard entities/examples in List I with their descriptions in List II.

List I: (Entity/Example)

P. Wintel
Q. GSM
R. Open Group
S. IETF

List II: (Description)

1. Promotes UNIX and the like
2. Combination of Microsoft OS and Intel microprocessor
3. Created the first standards of SMTP and TCP/IP
4. Adopted as a government standard for phones

(A) P-2, Q-4, R-1, S-3
(B) P-4, Q-1, R-3, S-2
(C) P-2, Q-3, R-4, S-1
(D) P-1, Q-2, R-3, S-4

**Oct/Nov 2017**

**103.** The following question consists of two statements — Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.

Assertion (A): Demo software is primarily designed to demonstrate what a purchased version is capable of doing, often functioning like an automated tutorial.

Reason (R): Demo software is intended to be a fully functioning program that completely replaces the need for retail software.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2019**

**104.** Consider the following rights that a copyright holder of software typically possesses:

I The right to reproduce copies of the work.
II The right to adapt the work by creating derivative works.
III The right to distribute copies of the work by sale or lease.
IV The right to regulate access to the source code.
V The right to forcibly extract source code from public domain software.

Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (IV)
(B) (II), (III), (IV), and (V)
(C) (I), (III), (IV), and (V)
(D) (I), (II), (IV), and (V)

**Oct/Nov 2006**

**105.** XYZ Financials experienced a catastrophic server failure resulting in the corruption of several critical client databases. Fortunately, the IT department had deployed a specialized software routine that allowed them to specify exactly what files were copied daily, preserving the original organization of files, and ensuring easy retrieval.

Which specific category of software saved XYZ Financials?
(A) Graphical user interface utilities
(B) Retail CRM software
(C) Data backup and recovery software
(D) Firmware hypervisors

**May/June 2006**

**106.** Match the third-generation programming languages in List I with their descriptions in List II.

List I: (Programming Language)
P. Java
Q. Ruby
R. Perl
S. COBOL

List II: (Description)
1. Very verbose, designed so commands describe in English exactly what is being done
2. Designed for portability using a virtual environment (JVM)
3. Synonymous with "CGI scripting", thriving on text-processing abilities
4. Pure object-oriented language with clearer syntax, leaving behind shortcomings of other languages

(A) P-2, Q-4, R-3, S-1
(B) P-4, Q-2, R-1, S-3
(C) P-1, Q-3, R-2, S-4
(D) P-2, Q-1, R-4, S-3

**Oct/Nov 2009**

**107.** Which of the following statements incorrectly represents the OSI criteria for an 'Open Standard'?

(A) The standard must not withhold any detail necessary for interoperable implementation.
(B) The standard must define a process for fixing flaws identified during implementation.
(C) The standard must require execution of a strict non-disclosure agreement (NDA) before access is granted.
(D) All patents essential to implementation must be licensed under royalty-free terms for unrestricted use.

**May/June 2014**

**108.** Consider the following statements about Shared Source arrangements:

I They are identical in definition and legal framework to Open Source Software (OSS).
II They allow limited sharing of proprietary source code with an identified group of customer representatives.
III The Microsoft Windows Shared Source

Click Here to Buy book on Amazon

Initiative is a well-known example.
Which of the above statement(s) is/are correct?
(A) (I) and (II)
(B) (II) and (III)
(C) (I) and (III)
(D) (I), (II), and (III)

**Oct/Nov 2012**

**109.** The following question consists of two statements — Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): In most cases, machine language can be converted back into a form of source code using a de-compiler.
Reason (R): A de-compiler perfectly reverses the compilation process, recovering all original human-readable comments and variable names without any imperfections.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2009**

**110.** Consider the following statements regarding OEM software:
I OEM stands for Original Equipment Manufacturer.
II It is software sold in bulk to resellers, designed to be bundled with hardware.
III Microsoft sells its operating systems as OEM software at a reduced price.
IV OEM software usually lacks retail packaging and printed installation instructions.
V It is perfectly legal to buy OEM software unbundled from its original hardware system.
Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (IV)
(B) (II), (III), (IV), and (V)
(C) (I), (III), (IV), and (V)
(D) (I), (II), (IV), and (V)

**Oct/Nov 2007**

**111.** An architectural firm wants to create high-quality 3D printed models of their new building designs. To keep overhead costs low, they search for an open-source 3D computer graphics software developed by an Amsterdam-based foundation.
Which of the following software platforms would meet their operational requirement?
(A) VirtualBox
(B) MySQL
(C) PHP
(D) Blender

NODIA

**May/June 2017**

**112.** Match the Operating Systems in List I with their context in List II.
List I: (Operating System)
P. MS-DOS
Q. Windows NT Server
R. Windows 11
S. Windows 2022
List II: (Context)
1. Designed to act as a server in networks
2. Latest version for servers
3. Standard operating system shipped on most Intel architecture personal computers in the 1980s
4. Latest version for desktops
(A) P-3, Q-1, R-4, S-2
(B) P-1, Q-3, R-2, S-4
(C) P-3, Q-2, R-1, S-4
(D) P-4, Q-1, R-3, S-2

**Oct/Nov 2025**

**113.** Consider the following statements about Web Browsers:
I They are exclusively intended to access private network files without Internet capability.
II They consist of a user interface, layout engine, Javascript interpreter, and networking components.
III Safari holds a larger market share than Mozilla Firefox as of December 2021.
IV Internet Explorer was deprecated in Windows 10, replaced by Microsoft Edge.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (III)
(B) (II), (III), and (IV)
(C) (I), (III), and (IV)
(D) (I), (II), and (IV)

**May/June 2008**

**114.** Which of the following is NOT listed as a strength of open source software?

(A) Free source code with no seat license fees
(B) High degree of dependency on overpriced open source consultants
(C) Agility giving deployments a competitive advantage in the marketplace
(D) Potential for code reuse reducing inefficiencies

**Oct/Nov 2008**

**115.** The following question consists of two statements — Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): An Open Standard must be freely and publicly available under royalty-free terms at reasonable and non-discriminatory cost.
Reason (R): Open Standards are fundamentally designed to create intentional secrets that protect corporate interoperability testing protocols.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2016**

**116.** Match the generation of languages in List I to its characteristics in List II.
List I: (Language Generation)
P. First Generation
Q. Second Generation
R. Third Generation
S. Fourth Generation
List II: (Characteristic)
1. Uses mnemonic operation codes and symbolic addresses
2. Also known as high-level languages, appearing much like everyday text and mathematical formulas
3. Consists of ones and zeroes; painfully difficult to work with
4. Non-procedural languages needing approximately one-tenth the statements of high-level languages
(A) P-3, Q-1, R-2, S-4
(B) P-1, Q-3, R-4, S-2
(C) P-2, Q-4, R-1, S-3
(D) P-3, Q-2, R-1, S-4

**Oct/Nov 2013**

**117.** Open standards are characterized by all of the following EXCEPT:
(A) They are publicly available technical specifications.
(B) They are without individual vendor restrictions on access.
(C) They are developed or affirmed in a collaborative or consensus-based process.
(D) They must be implemented exclusively by open source software.

**May/June 2015**

**118.** Consider the following statements representing the weaknesses of open source software:
I There is often no control over an open source project's development schedule.
II It requires no in-house staff to stay up to date with platform issues.
III New versions must be integrated and compatible, creating an ongoing challenge.
IV Open source quality can vary dramatically.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (III)
(B) (II), (III), and (IV)
(C) (I), (III), and (IV)
(D) (I), (II), (III), and (IV)

**Oct/Nov 2012**

**119.** Which of the following statements correctly describes Natural Languages (Fifth Generation)?
(A) They strictly enforce mathematical syntax and reject any misspelled words.
(B) They are low-level languages used explicitly for assembling object codes.
(C) They prevent the computer from functioning without continuous internet bandwidth.
(D) The text of a natural language statement very closely resembles human speech.

**May/June 2020**

**120.** Consider the following conceptual steps of an API workflow:
I A client application makes an API call containing a request verb and headers.
II The API makes a call to the external program or web server.
III The API strictly bypasses all HTTP headers and cookies to increase speed.
IV The server responds to the API with the requested data.
V The data is returned to the original

Downloaded from www.pdf.tube

requesting application via the API.
Which of the above statement(s) is/are correct?
(A) (I), (II), IV), and (V)
(B) (I), (II), (III), and (IV)
(C) (II), (III), (IV), and (V)
(D) (I), (III), (IV), and (V)

**Oct/Nov 2015**

**121.** A massive legacy banking mainframe still processes millions of traditional financial transactions daily. The management decides to upgrade the system with object-oriented tools, but the codebase remains highly verbose, utilizing English-like commands such as "ADD SHIPPING-CHARGE TO INVOICE-SUBTOTAL".
Which programming language is the mainframe predominantly running?
(A) Ruby
(B) Perl
(C) Python
(D) COBOL

**May/June 2018**

**122.** A web developer is troubleshooting a webpage that loads text perfectly but fails to apply the interactive formatting and CSS styles. The developer realizes the browser's internal mechanism responsible for transforming the markup into an interactive document is stalling.
Which component of the web browser is experiencing the failure?
(A) The networking component
(B) The data persistence component
(C) The layout/rendering engine
(D) The UI backend

**Oct/Nov 2014**

**123.** An employee downloads a free multimedia player to listen to music at work. Unbeknownst to the employee, the software covertly profiles the music and video files played, associates them with a unique identification tag on the employee's machine, and transmits this data back to a third-party server without consent.
What specific category of software behavior does this represent?
(A) System diagnostic utility
(B) Public domain telemetry
(C) Spyware
(D) OEM benchmarking

**May/June 2010**

**124.** A user clicks on a link intended to open an obscure, unsupported proprietary engineering schematic file within Google Chrome. Instead of displaying the schematic in the browser window, a dialog box immediately appears asking where to store the file locally on the computer.
Why did the browser behave in this manner?
(A) The browser prompts the user to save the file when it is an unsupported type.
(B) The layout engine crashed while attempting to render the complex HTML content.
(C) The file was flagged as a potential spyware threat by the browser's security.
(D) The file requires a partner API key to be displayed within the window frame.

**Oct/Nov 2005**

**125.** A junior programmer is overwhelmed by typing multiple command-line prompts for compiling, interpreting, and debugging their code sequentially. A senior developer advises them to install a software bundle that merges all these tools into a single advanced graphical user interface, eliminating the need to type individual compilation commands.
What type of software bundle did the senior developer recommend?
(A) An operating system kernel
(B) An Integrated Development Environment (IDE)
(C) A Fifth Generation Language Natural Interpreter
(D) A database management system

NODIA

www.nodia.in

# ANSWERS

1. (D) To insulate application programs from the complex operational details of the underlying hardware
System software acts as a layer of abstraction that manages the communication between hardware components and user applications. By handling complex low-level operations such as memory management and hardware interfacing, it provides a stable environment for other programs. This insulation allows application developers to focus on functionality without worrying about the specific technical details of the underlying computer hardware.

2. (C) It bridges the gap between assembly language efficiency and high-level structural convenience.
The C programming language is valued for bridging the gap between high-level language convenience and the performance of low-level assembly code. It offers powerful features like pointers for direct memory manipulation while maintaining a structured syntax. This unique balance makes it an ideal choice for developing efficient operating systems and applications that require high performance across diverse hardware architectures.

3. (C) Binary value groups representing processor instructions that change the computer state
Machine language serves as the native tongue of a computer's processor, consisting of binary code that the hardware executes directly. These instructions are represented as groups of ones and zeros, which command the CPU to perform specific tasks. Because it is tied to the physical design of the processor, machine language varies significantly between different types of computer architectures.

4. (C) Software that allows end users to accomplish one or more specific non-computer related tasks
Application software is designed to help users perform specific tasks that address real-world needs rather than computer maintenance. Programs like word processors, spreadsheets, and media players fall into this category. By utilizing the underlying system software to communicate with hardware, these applications provide a user-friendly interface for accomplishing various productive, creative, or entertainment-related activities on a computer.

5. (B) Linux is utilized by more than 95% of the top 1 million servers on the planet.
Linux is a dominant force in the server market due to its stability, security, and open-source nature. Statistics reveal that it is utilized by more than ninety-five percent of the top one million servers globally. Its efficiency in handling cloud infrastructure and high-traffic web environments makes it the preferred choice for major technology companies and data centers worldwide.

6. (B) It tracks an organization's goods and materials on the basis of quality as well as quantity.
Inventory management software is a specialized application used by organizations to monitor their supply of goods and materials. It tracks items based on both quantity and quality, ensuring that stock levels are maintained efficiently. This software helps businesses optimize their warehouse operations, improve customer service by ensuring product availability, and manage the movement of materials throughout the entire supply chain.

7. (B) A set of programs, procedures, and documentation for performing tasks on a computer system
Computer software is broadly defined as the collection of instructions and data that tell a computer how to work. It encompasses programs, the procedures used during execution, and the documentation required to understand or operate the system. Unlike the physical hardware components, software is intangible and provides the logical framework necessary for the computer to perform any meaningful task.

8. (B) It uses binary patterns of ones and zeroes that digital processors execute as instructions.
Machine language is unique because it is the only language that digital processors can interpret and execute directly without any prior translation.

Click Here to Buy book on Amazon

It consists of patterns of binary digits that correspond to specific hardware instructions. While human-readable high-level languages require compilers or interpreters to function, machine language communicates with the computer's circuitry at the most basic electrical level.

**9.** (A) Only (I)
Visual Basic was developed as a versatile tool that combines the simplicity of the BASIC language with advanced features for rapid application development. It also incorporates elements from Microsoft Office macro languages, allowing for easy automation within professional suites. This combination provides developers with a powerful environment for creating Windows-based applications and macros that streamline complex workflows across various platforms.

**10.** (C) Android
In the global mobile market, Android has established itself as the leading operating system by share of users. Its open-source foundation allows multiple manufacturers to produce a wide variety of devices at different price points. This flexibility and accessibility have contributed to its widespread adoption, surpassing competitors like iOS and Windows Phone to become the most used mobile platform worldwide.

**11.** (D) It is legal to buy unbundled from its original hardware system.
Original Equipment Manufacturer software is specifically produced to be bundled with hardware devices by computer manufacturers. It is typically sold in bulk to resellers and usually excludes retail items like fancy packaging or printed manuals. In many legal jurisdictions, it has been established that it is legal to buy and use OEM software unbundled from its original hardware system, even if license agreements state otherwise.

**12.** (C) Middleware software
Software in modern computer systems is generally categorized into three major classes: system software, programming software, and application software. System software manages the hardware, while programming software helps developers create new tools. Application software performs specific tasks for users. Middleware, while important for connecting different software components, is not considered one of these three primary foundational classes of software.

NODIA

**13.** (A) Fortran
Third-generation languages improved programming by using human-readable syntax. Many of these, such as Java, C++, and Ruby, are designed around object-oriented principles, allowing for modular and reusable code. Fortran, however, is a much older language primarily used for scientific and mathematical processing. While it has received many updates over the years, it is not traditionally classified as an object-oriented language.

**14.** (A) (II), (III), (I)
The history of the UNIX operating system is defined by a specific sequence of programming language developments. BCPL was the earliest language in this lineage, followed by the development of the B language. These eventually led to the creation of the C language, which provided the efficiency and features needed for UNIX. This chronological order marks a significant era in software development.

**15.** (D) Computer Hardware
In the hierarchical model of a computer system, layers of software and hardware interact to perform tasks. The Systems Software layer, which includes the operating system, acts as an interface directly above the computer hardware. By managing the physical resources like the processor and memory, this layer provides a stable foundation for the application software that sits further up the stack.

**16.** (A) Software is loaded into RAM and executed by the CPU through machine language instructions.
Software interacts with hardware at the lowest level by loading instructions into the random access memory. The central processing unit then fetches and executes these machine language commands to perform logical and mathematical operations. This process allows the abstract instructions written by programmers to be converted into physical signals that change the electrical state of the computer's hardware components.

17. (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Fifth Generation Languages represent a significant evolution where programmers focus on defining the problem and its constraints rather than writing step-by-step algorithms. These languages are designed to let the computer solve the problem automatically based on the logic provided. This declarative approach allows for the development of complex artificial intelligence systems and database queries without needing to implement detailed routines.

18. (A) A program that organizes computer functions, manages jobs, and assigns them to proper locations
An operating system is a fundamental type of system software that coordinates all the activities of a computer. It manages hardware resources, organizes various functions, and assigns tasks to the appropriate locations for execution. By providing a consistent interface for users and applications, the operating system ensures that the computer functions efficiently and that all hardware components communicate correctly with each other.

19. (D) Java - Designed for portability utilizing a virtual environment
Java is widely recognized for its “write once, run anywhere” philosophy, which is achieved through its high portability. It runs programs within a specialized virtual environment known as the Java Virtual Machine. This allows the same code to execute on different operating systems without modification, making it a powerful tool for developers creating applications that must function across diverse hardware platforms.

20. (A) A software bundle merging text editors, compilers, and debuggers into a single interface
An Integrated Development Environment is a comprehensive software suite that combines all the essential tools for software development into one user interface. It typically includes a text editor for writing code, a compiler for translation, and a debugger for fixing errors. By merging these components, an IDE streamlines the development process, allowing programmers to manage their projects more efficiently.

21. (C) It performs a broad range of highly complex, organization-wide financial tasks.
Utility software, often called service routines, consists of specialized programs designed to help manage and maintain computer hardware and other software. Common examples include disk defragmenters and virus scanners. Unlike enterprise application software, utility programs do not perform complex organization-wide financial tasks. Instead, they focus on small, specific maintenance jobs that keep the computer system running smoothly and securely.

22. (B) Word processors
System software includes programs that manage and support the operation of a computer. Key examples are operating systems, device drivers, and diagnostic tools, which ensure hardware and software work together effectively. Word processors, however, are categorized as application software because they are designed to perform specific user tasks, such as creating documents, rather than managing the internal functions of the computer.

NODIA

23. (A) Only (I)
Windows NT was developed as a powerful operating system designed for high-performance and network environments. A key feature of this system is its support for pre-emptive multitasking, which allows it to manage multiple programs simultaneously by giving the processor control over task switching. This capability ensured greater stability and efficiency, making it a reliable choice for both workstations and server deployments.

24. (C) (I) and (III)
Fourth Generation Programming Languages are non-procedural tools that allow developers to specify what the computer should achieve without detailing every step of how to do it. These languages are highly efficient, often requiring much fewer statements than high-level languages. They are frequently used alongside databases and data dictionaries, enabling users to generate reports and queries quickly and with minimal effort.

**25.** (B) They are highly portable and easily converted to run on any architecture without modification.
Assembly languages provide a low-level interface by using symbolic mnemonics to represent machine code instructions. While they allow for highly efficient and fast programs, they are not easily portable. Because they are designed for the specific architecture of a particular processor, code written for one system cannot be moved to another without significant changes to account for hardware differences.

**26.** (D) High-level languages are compiled or interpreted into machine language object code.
High-level programming languages are designed to be human-readable, using words and mathematical symbols that are familiar to developers. However, these languages cannot be executed directly by a computer's hardware. Instead, they must be translated into machine language object code. This process is handled by a compiler or an interpreter, which converts the high-level syntax into binary instructions for the CPU.

**27.** (A) MSOffice Suite
General application software consists of programs designed to perform a wide variety of tasks for the end user. The Microsoft Office Suite is a prime example, offering tools for word processing, spreadsheet creation, and presentations. Unlike system-level utilities or operating system kernels, these applications are focused on providing specific functionalities that help users accomplish productive tasks in their daily lives.

**28.** (B) (II), (III), (I)
The evolution of Microsoft Windows began with its release as a graphical operating environment that ran on top of MS-DOS. Later, Windows 95 used MS-DOS primarily as a bootstrap to start the system. Eventually, the operating system matured to the point where Windows 7 overtook Windows XP to become the most commonly used version for personal computers and business environments.

**29.** (C) COBOL - Primarily used for complex scientific and mathematical optimization
Programming languages are developed for specific use cases and environments. Python is known for being open-source and object-oriented, while Perl is famous for text processing. COBOL, however, was designed specifically for business and financial applications rather than complex scientific or mathematical optimization. For high-level scientific and mathematical tasks, languages like Fortran or specialized libraries are typically used instead of COBOL.

**30.** (A) P-3, Q-1, R-4, S-2
Different operating systems have unique origins and characteristics. HP-UX is a descendant of System V Unix for specific hardware, while macOS is a BSD-based variant. Solaris is notable for its ability to run on multiple types of hardware including x86 servers. Linux is a free UNIX-like system that is highly popular in academic environments and widely used across diverse architectures.

**31.** (C) A Software Escrow Arrangement
A software escrow arrangement is a contractual agreement where a neutral third party holds the source code of critical software. If the developer goes out of business or fails to provide support, the escrow agent releases the code to the customer. This provides businesses with a safety net, ensuring they can maintain their operations even if their software vendor fails.

**32.** (B) (I), (III), (IV), and (V)
Organizations choose open source software for several strategic reasons. These include lower costs due to the absence of licensing fees and increased security through transparent code review. Furthermore, open source avoids vendor lock-in, allowing companies to switch providers more easily. Many users also believe that the collaborative nature of open source development leads to better quality and more reliable software products.

**33.** (D) (I), (II), (III), and (IV)
Spyware is a type of malicious software designed to gather data from a computer without the user's consent. It is commonly classified into several categories, including adware that displays unwanted commercials and system monitors that track activity. Other forms include tracking cookies that monitor web usage and trojans that provide unauthorized access to a system while appearing as legitimate software.

Downloaded from www.pdf.tube

**34.** (D) Opportunities
Building commercial software on top of existing open source platforms allows startups to enter the market quickly and at a lower cost. This strategy leverages the opportunities provided by the open source model, such as access to robust, pre-existing codebases and external developer expertise. By focusing on customization rather than basic development, companies can launch products faster and more efficiently.

**35.** (A) All open source software is universally covered by the GNU General Public License (GPL).
Open source software is governed by various licenses, and not all are covered by the GNU General Public License. The Open Source Initiative identifies numerous licenses that meet the standard for being "open source." Some licenses allow developers to modify and use the code without being required to share their new versions with the general public under the same terms.

**36.** (A) It must not prohibit conforming implementations in open source software.
The Open Source Initiative mandates that an open standard must not place restrictions that prevent the standard from being implemented within open source software. This ensures that developers can create conforming implementations without facing legal or technical barriers. Such a requirement promotes a level playing field where both proprietary and open source technologies can coexist and interoperate using the same specifications.

**37.** (A) It permits a free trial for a set period, after which it must be purchased or uninstalled.
Shareware is a software distribution model that allows users to try a program for a limited time before purchasing it. After the trial period ends, the user must buy a license to continue using the software legally or uninstall it. This "try before you buy" approach helps users evaluate the software's features and compatibility before making a financial commitment.

**38.** (A) Only (I)
Python is a highly versatile, open-source programming and scripting language widely used for web and mobile development, as well as video games. PHP, however, is a server-side scripting language primarily used for web development rather than being a relational database management system. Therefore, only the statement regarding Python's use in various application types and its open-source status is correct.

**39.** (D) Strengths
Shifting to an open source environment offers significant strengths for an organization, such as agility and the freedom to modify code without paying for individual seat licenses. The rapid release of patches and the ability to customize software to meet specific needs provide a competitive advantage. These benefits allow businesses to deploy solutions quickly and maintain control over their infrastructure.

**40.** (D) The licensor is usually required to update the source code as the software package is upgraded.
In a software escrow agreement, it is crucial that the materials held by the agent remain current. Generally, the licensor is required to update the source code with the escrow agent whenever the software package undergoes significant upgrades or updates. This ensures that the customer always has access to the most recent version of the code if a release trigger occurs.

**41.** (D) The patents must demand a standard royalty fee from all open source implementations.
For a technology to be considered an open standard by the Open Source Initiative, any essential patents must be licensed on a royalty-free basis. The standard must not demand any royalty fees or financial compensation from those who implement it. This requirement ensures that both open source and proprietary developers can create compatible software without facing prohibitive costs or restrictions.

**42.** (B) (I), (II), (III), and (IV)
The GNU General Public License is built on four fundamental freedoms that protect the rights of software users. These include the freedom to run the program for any purpose, study its inner workings, and redistribute copies to others. Additionally, users are encouraged to improve the program and release those improvements to the general public, ensuring the software remains open and collaborative.

NODIA

**43.** (B) (II) and (III)
LibreOffice and VirtualBox are popular tools in the open-source community. LibreOffice is recognized for including advanced features like a QR code generator for mobile links. VirtualBox, developed by Oracle, is a hosted hypervisor used for x86 virtualization. Together, these applications provide powerful functionality for document management and running multiple operating systems on a single computer for testing and development.

**44.** (D) Redistribution of the code or sharing with third parties
Shared source arrangements allow organizations to review the source code of proprietary software under specific protective conditions. While this permits limited sharing with identified customers, governments, and educational institutions for security audits or learning, it does not allow the code to be redistributed. Sharing the code with third parties or the general public is strictly prohibited under these types of agreements.

**45.** (C) The Motion Picture Engineering Group compression standard (MPEG).
The Motion Picture Engineering Group compression standard, commonly known as MPEG, is a well-known example of an open standard used in electronic commerce and media. These standards provide a common set of specifications that allow different software and hardware to handle digital video and audio consistently. This interoperability is essential for the global distribution of digital content across various platforms and devices.

**46.** (A) P-4, Q-1, R-3, S-2
Different software types are defined by their licensing and functionality. Crippleware has key features disabled after a trial. Demo software acts as an automated tutorial for the full version. Adware is supported by integrated advertisements. Spyware covertly transmits user data to external servers. Understanding these categories helps users manage their privacy and software expectations when downloading programs from the internet.

**47.** (B) Spiraling maintenance threats
One risk of relying on niche open-source projects is the possibility that the core contributors will stop maintaining the code. If a project is abandoned, users may face spiraling maintenance threats, including a lack of technical support and increased costs for managing the software themselves. This situation can lead to schedule overruns and potential security vulnerabilities as the codebase becomes outdated.

**48.** (B) The agent has no liability in relation to the release and use of the source code.
In a standard software escrow agreement, the independent agent acts as a secure custodian of the source code. If the agent fulfills its duties to keep the materials confidential and secure, it generally bears no liability regarding how the code is used by the customer after release. The responsibility for the software's operational performance remains with the original developer and the user.

**49.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
The growth of the open source software model is deeply connected to the rise of the modern Internet. As a global communications network, the Internet provides the necessary infrastructure for developers around the world to collaborate on code, share improvements, and host projects. This connectivity has enabled open source communities to thrive and produce high-quality software through collective international effort.

**50.** (A) P-3, Q-1, R-4, S-2
Open-source software provides various tools for everyday tasks. GIMP is a powerful image editor, while Mozilla Firefox is a widely used web browser. The GNU project provides a collection of software that forms a UNIX-like operating system. VLC is a versatile multimedia player capable of handling many file formats. These applications offer high-quality, free alternatives to many well-known proprietary software products.

**51.** (D) The standard must define a process for fixing flaws and incorporate changes into revised versions.
The 'No Intentional Secrets' requirement for an open standard ensures that all details necessary for interoperability are publicly disclosed. Additionally, the standard must define a clear process for identifying and fixing flaws, which

Click Here to Buy book on Amazon

# STUDYING FROM PDFs?

# THINK AGAIN.

If you are studying only from PDFs,
you are wasting valuable time.

Research shows that learning from

**PRINTED BOOKS** has up to

**4× HIGHER RETENTION**

than studying from screens.

**PRINT BOOK = BETTER MEMORY**

**PDF = LOWER RETENTION**

Those who study from **PRINTED BOOKS**
move **AHEAD.**

Others are left **BEHIND**
in competition.

In competitive exams,
being average is not enough.

## STAY ONE STEP AHEAD.

are then incorporated into revised versions of the specification. This transparency prevents creators from withholding information and ensures that all developers can create fully compatible software implementations.

**52.** (C) Assertion (A) is true, but Reason (R) is false.
The GNU General Public License allows distributors to charge a fee for the service of providing the software and support. The term "free" in the GPL refers to liberty and user rights rather than the absence of cost. Therefore, it is perfectly legal to sell a distribution of GPL software, even though the underlying license grants users the freedom to modify it.

**53.** (C) Commercial software can be open source, so equating commercial with proprietary is incorrect.
It is a common misconception that all commercial software is proprietary. Commercial software is simply software produced for sale or business purposes, and it can be open source or closed source. Proprietary software refers specifically to programs where the source code is kept private. Therefore, equating the two is incorrect, as many companies successfully sell products based on open-source code.

**54.** (C) Weaknesses
Using open source software can sometimes lead to unexpected challenges for businesses. A common weakness is the rapid rate of new version releases, which can overwhelm internal IT staff. If a company cannot keep up with these updates, they may be forced to hire expensive external consultants, potentially negating some of the cost savings associated with using free open-source software platforms.

**55.** (D) (I), (II), and (III)
Several major open-source projects have shaped the modern digital landscape. Blender is a leading tool for 3D graphics, while MySQL is a critical database component used in the LAMP stack for e-commerce. Linux, originally created by Linus Torvalds, is a foundational operating system released under the GPL. Together, these technologies provide powerful and reliable solutions for developers and organizations worldwide.

**56.** (A) Public domain software is the only type users can legally modify for their own purposes.
Public domain software is unique because it is not protected by copyright and has no legal owner. This status allows users the complete freedom to modify, distribute, and use the code for any purpose without seeking permission. While other types of software like freeware or shareware may be free to use, they still have copyright restrictions that typically prohibit modification.

**57.** (A) Public technical specifications developed via consensus without vendor limits.
Open standards are public technical specifications that are developed and maintained through a consensus-based process involving multiple stakeholders. They are designed to be available to everyone without individual vendor restrictions, promoting interoperability between different hardware and software products. By providing a common framework, open standards help prevent market fragmentation and ensure that technologies from different companies can work together.

**58.** (A) Source code is human-readable and must be translated into machine language for CPU execution.
Source code is the human-readable version of a program written in a programming language, while machine language is the binary code that a computer's processor actually executes. For software to run, the source code must be translated into machine language by a compiler or interpreter. This distinction is fundamental to understanding how developers write software and how hardware performs tasks.

NODIA

**59.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Proponents of open source software believe it is more secure because the source code is transparent and available for public review. This openness allows a global community of developers and security researchers to inspect the code for vulnerabilities and fix them quickly. Unlike closed-source software, where only the original developers see the code, open source benefits from many eyes finding flaws.

**60.** (B) An author or group that plays a key coordinating role in the software development project.
In the open source development model, a maintainer is an individual or a group responsible for coordinating the project's activities. They review contributions from other developers, decide which changes to incorporate into the main codebase, and manage the overall direction of the software. Their role is essential for maintaining code quality and ensuring that the project remains organized and productive.

**61.** (C) Firefox and Opera
Web browser compatibility is essential for a consistent user experience across different devices. Firefox and Opera are two browsers that offer versions for virtually all major operating systems, including Windows, macOS, Linux, and mobile platforms like Android and iOS. This wide availability ensures that users can access their favorite features and synchronized data regardless of the hardware or system they use.

**62.** (A) Internal API
An internal API is a private interface used within an organization to allow different software systems to communicate with each other. In this case, it enables a bank's HR and payroll software to share data securely on a private intranet. By blocking external access, the organization ensures that sensitive information remains protected while still allowing for efficient data integration between departments.

**63.** (B) P-3, Q-1, R-2, S-4
Open standards facilitate compatibility across different technology sectors. Hardware standards include USB and PCI, while file formats like HTML and PDF ensure consistent document display. Networking relies on protocols such as TCP/IP for communication. Programming languages like SQL and C provide standardized syntax for development. These standards work together to create an interoperable environment where diverse technologies can function seamlessly together.

**64.** (D) It prompts the user to save the file to disk rather than displaying it.
When a web browser encounters a file type that it cannot render, such as a specialized data file, it does not display the content. Instead, it typically prompts the user to save the file to their computer's hard drive. This allows the user to later open the file using a separate, compatible application that is designed to handle that specific format.

**65.** (A) It is a scripting language primarily used for web development that can be embedded in HTML.
PHP is a widely used open-source scripting language designed specifically for web development. It is particularly effective because it can be embedded directly into HTML code, allowing developers to create dynamic web pages and manage database content easily. PHP is a core component of many websites and web-based applications, providing the server-side logic needed for interactive online experiences.

**66.** (A) It provided a ubiquitous network for collaborative groups to host projects and maintain code versions.
The Internet played a vital role in the growth of open source development by providing a global platform for collaboration. It allowed developers to easily share code, host projects, and communicate with community members regardless of their location. This connectivity made it possible for large-scale software projects to be built and maintained by a distributed network of international volunteers.

**67.** (C) Compliance with royalty-free, freely available technical specifications.
The 'No Agreements' requirement for an open standard means that developers should not have to sign paperwork or non-disclosure agreements to implement it. However, they must still follow the royalty-free, publicly available technical specifications that define the standard. This approach ensures that anyone can create compatible software implementations without being burdened by legal hurdles or secret requirements during the development process.

**68.** (B) An Application Program Interface (API)
Application Program Interfaces provide significant security benefits by allowing sensitive information to be handled by specialized third-party services. In e-commerce, an API can transmit payment details to a processor that

Downloaded from www.pdf.tube

returns a secure token instead of storing the actual credit card data. This abstraction protects both the merchant and the customer by reducing the risk of sensitive data being compromised.

**69.** (C) It transforms HTML and associated content from mark-up into an interactive web document.
A layout or rendering engine is a core component of a web browser that processes HTML, CSS, and images to display them as a graphical web page. It takes the underlying code and formatting instructions and transforms them into the interactive document that users see on their screens. This ensures that web content is presented consistently and correctly across different websites.

**70.** (C) Prefixes the browser cannot handle are ignored and generate an error screen.
URL prefixes tell a browser how to interpret and fetch a resource. The 'file:' prefix is for local files, and 'news:' is for newsgroups. If a browser cannot handle a prefix, it will be ignored and the software will generate an error screen for the user. This indicates that the browser does not have the necessary protocol support or configuration to access the requested resource.

**71.** (A) Solving a problem based on conditions without writing a routine or algorithm.
Fifth Generation Programming Languages allow users to solve problems by defining goals and constraints rather than writing step-by-step instructions. This approach is often used in artificial intelligence and complex database systems. By focusing on "what" needs to be solved instead of "how" to solve it, these languages enable the computer to automatically determine the most efficient path to the solution.

**72.** (B) Software that lets users visit web pages on the Internet or access information on private networks.
A web browser is a software application that allows users to access and view information on the Internet or private networks. It retrieves content from servers and renders it into human-readable pages, including text, images, and videos. By providing a user-friendly interface and support for various protocols, browsers have become the primary tool for navigating the vast resources available online.

NODIA

**73.** (C) Partner API
A partner API is a specialized interface that is only accessible to authorized business partners. In this scenario, the airline provides a dedicated connection to a hotel booking service, requiring a formal onboarding process and secure credentials. This allows the two companies to share specific data and services securely, facilitating strategic collaborations while maintaining control over who can access the information.

**74.** (C) A piece of code that enables two software programs to communicate
At its core, an Application Program Interface is a set of rules and code that allows two different software programs to communicate and share data with each other. It acts as a bridge, enabling developers to integrate various services and functionalities into their own applications without needing to understand the complex internal workings of the other software products involved.

**75.** (D) Managing relational database data warehousing systems
Blender is a versatile open-source software package used primarily for 3D modeling, animation, and visual arts. It is also used to create models for 3D printing and to give the global community access to high-quality 3D technology. However, it is not designed for managing relational database systems or data warehousing, which are tasks handled by specialized database software.

**76.** (D) The widely accepted combination of Microsoft operating systems and Intel microprocessors.
Wintel is a term used to describe the dominant standard for personal computers that combines Microsoft Windows operating systems with Intel microprocessors. For decades, this combination has defined the architecture of most PCs, providing a consistent platform for developers and users. This widespread adoption created an industry standard that influenced the design of hardware and software across the global technology market.

**77.** (D) It is a required component of the OS kernel needed for system booting.
Inventory management software is a vital tool for tracking goods and materials based on their

quantity and quality within an organization. It helps businesses manage warehouse movements and optimize the flow of goods to improve customer service. While it is essential for business operations, it is an application-level program and is not part of the operating system kernel required for booting.

**78.** (D) It prompts the user to save the file to disk rather than displaying it.
If a web browser encounters a file format that it does not natively support, it will not try to render it. Instead, it provides the user with the option to download and save the file to their local hard drive. This ensures that the user can still access the content by opening it with a specialized application designed for that format.

**79.** (B) Assemblers convert mnemonics to object code; compilers translate high-level code.
An assembler is a low-level tool that converts mnemonic operation codes directly into machine language object code for a specific processor. In contrast, high-level language compilers translate complex, human-readable code into machine-executable instructions. While assemblers work closely with the hardware's native instruction set, compilers allow developers to write more abstract programs that can often be ported between different architectures.

**80.** (C) Assertion (A) is true, but Reason (R) is false.
APIs provide a valuable layer of abstraction that separates an application from the underlying services it uses. This decoupling allows developers to update or change their infrastructure without affecting the consuming applications. However, this does not mean that security is ignored; most APIs still require authentication and authorization to ensure that data is accessed safely and only by authorized users.

**81.** (C) They are machine-dependent, require hardware knowledge, and are not easily portable to other computers.
The primary reason assembly languages are not used for all programming is their lack of portability. Because they are tied to the specific instruction set of a particular processor architecture, code written in assembly for one type of computer cannot be easily run on another. This makes development more time-consuming compared to high-level languages, which can often run on many platforms.

**82.** (C) 65%
Google Chrome has grown to become the most popular web browser in the world, holding a dominant market share of approximately sixty-five percent as of December 2021. Its success is attributed to its speed, simple user interface, and deep integration with other popular Google services. This wide adoption has made it the primary target for web developers and designers.

**83.** (D) By bundling it with Windows, effectively funding it via OS sales to manufacturers and users.
Microsoft successfully funded the development and distribution of Internet Explorer by bundling it directly with its Windows operating system. By including the browser as a standard feature of the OS, Microsoft could leverage its massive market share to ensure the browser's widespread use. This strategy allowed them to fund the software through the sales of the operating system to manufacturers.

**84.** (B) Server hardware RAM allocation.
Rendering is the process by which a web browser takes web content and displays it on the screen. This involves processing HTML mark-up, CSS styles, and various image files to create a visual document. While this requires the use of local system resources like RAM, the browser does not manage the hardware RAM allocation of the remote server providing the content.

**85.** (C) Open (Public) API
An open API, also known as a public API, is an interface that is made freely available to developers over the internet. These APIs allow anyone to access specific data or services without needing formal contracts or complex authentication. This openness encourages innovation by allowing third-party developers to build new applications and services using the data provided by the original source.

**86.** (B) Only (II)
Open standards and open source software are distinct concepts that often work together. An open standard is a public specification for how a technology should work, while open source

Click Here to Buy book on Amazon

software is a program where the source code is available for anyone to modify. There is no requirement that an open standard must be implemented exclusively using open-source software products.

**87.** (B) It is much faster than applications written in compiled languages like C++.
Java is highly valued for its portability, which allows it to run on many different systems using a virtual environment. However, because it runs on a virtual machine rather than directly on the hardware, it is generally slower than compiled languages like C++. Despite this performance difference, Java's ease of use and cross-platform compatibility make it a popular choice for developers.

**88.** (D) Clicking a link forces the browser to restart the operating system to fetch the resource.
Web browsers navigate between resources using hyperlinks that contain the Uniform Resource Identifier of a specific target. When a user clicks a link, the browser retrieves and displays the indicated resource. This process allows users to jump between different pages and sites seamlessly. Clicking a link never forces the operating system to restart; it simply prompts the browser to fetch new information.

**89.** (B) It is a sequence of instructions for changing the state of computer hardware in a particular order.
Software is essentially a set of logical instructions that control how computer hardware operates. By providing a sequence of commands, software changes the internal state of the hardware to perform specific tasks. This allows the physical components of the computer, such as the processor and memory, to work together in a structured way to process data and produce meaningful results.

**90.** (B) (I) and (III)
The working of an API involves a simple exchange of information between a client and a server. A client application sends an API call with specific request details to a URI. The server processes this request and sends back the required data to the API. Finally, the API delivers this information to the original application, completing the transaction and sharing the data.

**91.** (B) Only (II)
The Open Standard Requirement for incompatible dependencies ensures that a standard remains truly open. It dictates that any technology required to implement the standard must also meet the criteria of being an open standard. This prevents proprietary technologies from being hidden within an open specification, ensuring that the entire system remains accessible and can be implemented by anyone without restrictions.

**92.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
APIs have become essential for modern web development because they allow different services to work together without needing to know each other's internal code. Developers can easily add features like maps or payment processing to their apps by communicating through these interfaces. This abstraction simplifies the development process and has led to a massive increase in the variety of web applications.

**93.** (A) P-3, Q-4, R-1, S-2
Open-source software provides diverse solutions for many technical needs. MySQL is a powerful database system used for e-commerce, while LibreOffice offers a full suite of office productivity tools. VirtualBox enables users to run multiple operating systems through virtualization, and PHP is a popular language for creating dynamic web content. Each of these tools plays a vital role in modern computing and development.

**94.** (C) It disables itself completely once the user's hard drive reaches full capacity.
Adware is a common type of software that is provided for free but displays advertisements to generate revenue for the developer. These programs often require an active internet connection to download and display new ads. While users may find the advertisements annoying, they are a condition of using the software for free. Adware does not disable itself based on hard drive capacity.

**95.** (D) (I), (II), (III), and (IV)
Fourth generation languages include several types of tools that help users work with data more efficiently. These include query languages for retrieving information from databases and report

Downloaded from www.pdf.tube

generators for creating structured documents. Other examples are application generators that help build new programs and decision support systems that analyze data to help businesses make informed choices. These tools simplify complex programming tasks significantly.

**96.** (B) Crippleware
Crippleware is a type of shareware that allows users to try a program, but with essential features like saving or exporting disabled. This strategy gives users a chance to test the software's interface and capabilities while requiring them to purchase a full license to perform any actual work. It is an effective way for developers to demonstrate their products.

**97.** (A) P-3, Q-1, R-4, S-2
Different software categories serve specific functions in a computer system. Utility software performs maintenance tasks like defragmentation, while data backup programs ensure that files can be easily recovered if lost. Retail software is sold in stores and usually includes manuals. Freeware is available for free download, often for personal use. Understanding these categories helps users choose the right tools for their needs.

**98.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Supercomputers require massive processing power and stability, which is why Unix and Unix-like systems are used in nearly all of these systems. Their efficient design and ability to handle complex tasks make them far more suitable for high-performance computing than other operating systems. As a result, the market share for Windows in the supercomputer sector is almost non-existent compared to Linux.

**99.** (B) It is the only software users can legally modify for their own purposes.
Public domain software is not protected by copyright, meaning that no individual or company owns the legal rights to the code. This gives users the unique freedom to modify, use, and redistribute the software in any way they choose. Because it lacks copyright restrictions, it is the only type of software that users can legally modify for any purpose they wish.

**100.** (B) (I) and (III)
Software licensing can be complex, but there are clear differences between various types. Freeware is free to use and should not contain malicious items like spyware. Crippleware refers to software where essential features are disabled to encourage a purchase, whereas software that stops working after a set time is known as trialware. Demo software, on the other hand, is usually just a limited version meant for evaluation rather than indefinite commercial use.

**101.** (A) LibreOffice
LibreOffice is a popular open-source alternative to proprietary office suites, known for its strong compatibility with Microsoft file formats. It includes several useful tools, such as a QR code generator that helps users create mobile-friendly links directly within their documents. This makes it a great choice for organizations looking to reduce costs without losing access to their existing files or advanced features.

**102.** (A) P-2, Q-4, R-1, S-3
Many entities have shaped the history of technology through standards and architectures. Wintel represents the long-standing combination of Microsoft software and Intel hardware. GSM was adopted as a global government standard for mobile phones. The Open Group promotes standards for UNIX, and the IETF was responsible for creating the original specifications for fundamental internet protocols like TCP/IP and email communication standards.

**103.** (C) Assertion (A) is true, but Reason (R) is false.
Demo software is designed to show potential buyers what the full version of a program can do, often through an automated presentation or tutorial. While it provides a good overview of the features, it is not intended to be a fully functional replacement for retail software. Instead, it serves as a marketing tool to encourage users to purchase the complete product.

**104.** (A) (I), (II), (III), and (IV)
Copyright holders have several exclusive rights to protect their software, including the right to reproduce it, create new versions, and sell copies. They can also control who gets to see the source code. However, these rights do not allow them to take control of software that is already in the

NODIA

public domain, as that code is free for everyone to use.

**105.** (C) Data backup and recovery software
Data backup and recovery software is essential for protecting important information from loss due to hardware failure or corruption. These programs allow users to schedule regular copies of their files and maintain their original organization, making it easy to retrieve them when needed. For businesses handling critical financial data, having a reliable backup system is a vital part of their operations.

**106.** (A) P-2, Q-4, R-3, S-1
Third-generation languages have different strengths based on their design. Java is built for portability across systems, while Ruby offers a clean, object-oriented syntax. Perl is widely used for text processing and web scripting. COBOL is a specialized language for business that uses English-like commands to perform tasks. Each of these languages has played a significant role in the development of modern software.

**107.** (C) The standard must require execution of a strict non-disclosure agreement (NDA) before access is granted.
To be considered an open standard by the Open Source Initiative, a specification must be transparent and accessible to everyone. This means that there should be no requirement to sign a non-disclosure agreement before being allowed to review or implement the standard. Such openness ensures that all developers can work on compatible implementations and that the technology remains truly public.

**108.** (B) (II) and (III)
Shared source arrangements allow companies to share their proprietary code with a select group of customers or partners for review. This is different from open source because the code cannot be freely redistributed. The Microsoft Windows Shared Source Initiative is a famous example of this model, allowing governments and large organizations to inspect the code for security and compatibility purposes.

**109.** (C) Assertion (A) is true, but Reason (R) is false.
A de-compiler is a tool that tries to turn machine language back into a human-readable form of source code. While it can often recover the basic logic of a program, it is not a perfect process. De-compilers cannot recover original variable names or the comments that developers write to explain their code, which are lost during the original compilation process.

**110.** (A) (I), (II), (III), and (IV)
OEM software is a version of a program that is designed to be sold alongside hardware by manufacturers. It is often cheaper than retail software but usually comes without fancy packaging or detailed manuals. While it is functional, the license often limits its use to the specific machine it was first installed on, though it remains a popular choice for computer builders.

**111.** (D) Blender
Blender is a high-quality, open-source 3D graphics software that is developed by a foundation based in Amsterdam. It is widely used for creating animations, visual arts, and models for 3D printing. Because it is free and powerful, it is an excellent choice for businesses and individuals who need professional-grade 3D tools without the high cost of proprietary software products.

**112.** (A) P-3, Q-1, R-4, S-2
Operating systems have evolved significantly over time to meet different needs. MS-DOS was the standard system for early PCs, while Windows NT was built for more powerful network server environments. Windows 11 is the latest version designed for modern desktop computers, and Windows Server 2022 provides the newest features for managing large-scale enterprise servers and network infrastructure.

**113.** (B) (II), (III), and (IV)
Web browsers are complex applications that combine a user interface with a layout engine and networking tools to display online content. While Chrome is the most popular, other browsers like Safari also hold a significant market share. Over time, older browsers like Internet Explorer have been phased out and replaced by more modern options like Microsoft Edge, which offer better performance.

Click Here to Buy book on Amazon

**114.** (B) High degree of dependency on overpriced open source consultants
Open source software offers many advantages, such as free access to source code and the ability to reuse and modify it to fit specific needs. These strengths provide businesses with agility and cost savings. However, a potential downside is the reliance on external consultants who may charge high fees, which is considered a weakness rather than a strength of the model.

**115.** (C) Assertion (A) is true, but Reason (R) is false.
Open standards are designed to be freely and publicly available to everyone under fair and non-discriminatory terms. This ensures that different companies can create products that work together without being hindered by secret or proprietary specifications. By avoiding intentional secrets, open standards promote a more open and competitive technology market where innovation can thrive for the benefit of all users.

**116.** (A) P-3, Q-1, R-2, S-4
Programming languages have evolved through different generations. First-generation languages used binary code, while the second generation introduced mnemonics for easier use. Third-generation languages are high-level and more like natural language. The fourth generation includes non-procedural languages that focus on results rather than steps. This progression has made it much easier for people to write complex programs and interact with computers.

**117.** (D) They must be implemented exclusively by open source software.
Open standards are technical specifications that are developed through a collaborative process and are available for anyone to use without vendor restrictions. While they are a key part of the open-source world, there is no requirement that they can only be used by open-source software. Both proprietary and free software can implement open standards to ensure they are compatible with other systems.

**118.** (C) (I), (III), and (IV)
Open source software has some weaknesses that organizations must consider. These include a lack of control over the development schedule and the challenge of integrating new versions that may have varying levels of quality. Additionally, companies must often have their own staff stay up to date with issues, which can be difficult if they do not have the right expertise in-house.

**119.** (D) The text of a natural language statement very closely resembles human speech.
Fifth-generation natural languages are designed to let people interact with computers using statements that very closely resemble human speech. These languages aim to make programming more accessible by allowing users to give commands in a more intuitive way. By reducing the need for strict mathematical syntax, they help bridge the gap between human communication and the complex logic of computer processing.

**120.** (A) (I), (II), IV), and (V)
An API works by following a clear series of steps to share data between applications. It begins when a client makes a call with specific request details. The API then contacts the external server, and once a response is received, the API delivers that information back to the original application. This process ensures that all headers and necessary information are handled correctly throughout the transaction.

**121.** (D) COBOL
COBOL is a long-standing programming language that is still widely used in the banking and financial industries for processing transactions on mainframes. It is known for its highly verbose syntax that uses English-like commands to perform calculations and manage data. This readability was originally designed to make the code easier for business professionals and auditors to understand and verify.

**122.** (C) The layout/rendering engine
The layout or rendering engine is the part of a web browser that is responsible for interpreting HTML and CSS to display a web page correctly. If this component fails, the text might load but the formatting and interactive elements will not work as intended. This engine is critical for ensuring that web content is presented to the user in a consistent way.

NODIA

**123.** (C) Spyware
Spyware is a type of software that secretly monitors a user's activities and transmits that data to an external server without their knowledge or consent. This can include tracking the files a person plays or their internet browsing habits. This behavior is a serious privacy concern, as it allows third parties to build profiles of individuals without their permission or awareness.

**124.** (A) The browser prompts the user to save the file when it is an unsupported type.
When a browser cannot display a certain file because it doesn't support that format, it will typically ask the user to save the file to their computer instead. This prevents the browser from crashing and gives the user a chance to open the file later with a more suitable program. It is a standard way for browsers to handle unsupported content.

**125.** (B) An Integrated Development Environment (IDE)
An Integrated Development Environment is a powerful tool for programmers because it combines a text editor, compiler, and debugger into one easy-to-use interface. This allows developers to write, test, and fix their code without having to switch between different programs or use complex command-line prompts. Using an IDE can greatly improve productivity and make the software development process much smoother.

www.nodia.in

Downloaded from www.pdf.tube

# CHAPTER 04
# Networking Systems

**May/June 2018**

**1.** An e-mail data communication system requires multiple integrated elements to set up a communication link and transmit data. Which of the following is NOT an essential component of this specific setup?
(A) Source and Destination Computers
(B) Data communication devices such as modems
(C) Specialized data communication software
(D) A dedicated physical firewall appliance

**Oct/Nov 2012**

**2.** An organization is evaluating on-line and off-line Internet connectivity. Which of the following factors fundamentally distinguishes an on-line connection from an off-line dial-up connection?
(A) On-line connectivity requires specific SLIP/PPP protocol software.
(B) Off-line connectivity utilizes a terrestrial leased line to an ISP.
(C) On-line connectivity provides flat-fee dedicated Internet access.
(D) Off-line connectivity prevents using modern graphical web programs.

**May/June 2005**

**3.** Which of the following statements correctly identifies a characteristic of a leased line in data communications?
(A) Its tariffs are based purely on the amount of data a user sends across the network.
(B) It is the most cost-effective alternative for mid-volume data transfers.
(C) It offers high performance because the line is permanently allocated by the telephone network.
(D) It provides highly flexible connections that the subscriber can alter dynamically without prior arrangement.

**Oct/Nov 2023**

**4.** A manufacturing company plans to install network cabling across its factory floor, which operates heavy machinery that generates massive electromagnetic interference. To ensure data integrity over extended distances, which of the following transmission media must the company implement?
(A) Unshielded Twisted Pair (UTP)
(B) Thin-net Coaxial Cable
(C) Optical Fiber Cable
(D) Thick-net Coaxial Cable

NODIA

**May/June 2011**

**5.** Consider the following statements regarding Internet Connectivity:
I The wired connections use PSTN/PSDN terrestrial links for connectivity.
II The wireless connection for wide area connectivity is achieved primarily through satellite communications.
III Private organizations are prohibited from providing E-mail and Internet services in India.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

**Oct/Nov 2007**

**6.** Which conceptual distinction accurately separates Radio transmission from Microwave transmission?
(A) Radio waves travel in omni-directional patterns, whereas microwaves need aligned antennas.
(B) Radio waves penetrate buildings, whereas microwaves travel in straight lines.
(C) Radio transmission operates in the infrared spectrum, whereas microwaves use visible light.
(D) Radio waves are unaffected by rain, whereas microwaves are severely absorbed at low frequencies.

May/June 2024

**7.** Electronic Mail (E-mail) systems primarily operate on which of the following principles to deliver messages to recipients?
(A) Real-time synchronous delivery directly to the recipient's local hard drive
(B) A store and forward basis utilizing a mailbox located in a computer
(C) Continuous peer-to-peer transmission until the receiving node acknowledges receipt
(D) Direct point-to-point analog switching without intermediate storage

Oct/Nov 2014

**8.** Which of the following is a correct statement regarding the replacement of dial-up Internet access by broadband?
(A) Broadband connections require the exclusive use of a phone line for data transmission.
(B) Broadband connections typically offer speeds of 700 kbit/s or higher.
(C) Dial-up access currently dominates the global market due to its always-on capability.
(D) Broadband forces the user to manually disconnect at the end of each session to save bandwidth.

May/June 2010

**9.** Local Area Networks (LANs) are characterized by several specific operational features. Which of the following is NOT a characteristic of a LAN?
(A) The network is confined to a small area typically a single building or cluster of buildings.
(B) The network utilizes a widely dispersed, non-shared public transmission medium.
(C) The data rate on the network is high, ranging anywhere from 10 Mbps to 10 Gbps.
(D) The devices on the network act as peers, meaning any device can initiate data exchange.

Oct/Nov 2020

**10.** Which of the following best describes why a dial-up line becomes uneconomical for large data transfers above a certain volume threshold (n1)?
(A) The physical copper conductors degrade under sustained high-frequency signaling.
(B) Telephone companies automatically switch the connection to a leased line tariff.
(C) The slow speed of the dial-up line directly inflates the time-based call charges.
(D) Packet switching networks forcibly throttle dial-up bandwidth to prevent congestion.

May/June 2016

**11.** Consider the following statements about coaxial cables:
I Thick-net translates an increase in size into an increase in maximum effective distance at the expense of flexibility.
II Thin-net is primarily used as the network backbone, with thick-net serving as the branches to individual network components.
Which of the above statement(s) is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

Oct/Nov 2009

**12.** A corporation needs to transfer a mid-volume range of data between two geographically remote offices. Based on cost comparisons, which data communication solution would be the most cost-effective choice for this specific volume?
(A) A standard dial-up line
(B) A dedicated leased line
(C) A Packet Switching Network (PSN)
(D) A Very Small Aperture Terminal (VSAT)

May/June 2023

**13.** Consider the following statements regarding the application of Intranets in corporate environments:
I They facilitate easiness in process integration across mobile sales forces and supply management.
II They integrate information systems with human resources management and corporate finance.
III They are strictly limited to providing email services and do not support Web browsers.
IV They play a significant factor in the digital economy by managing distributed corporate information.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (III) only
(B) (I), (III), and (IV) only
(C) (I), (II), and (IV) only
(D) (II), (III), and (IV) only

Click Here to Buy book on Amazon

Oct/Nov 2018

**14.** Which of the following definitions most accurately describes an Intranet?
(A) A global network system that is accessible to all registered users worldwide.
(B) An external system allowing trusted outside users to access internal resources.
(C) A closed network using internet technology to manage corporate data.
(D) A wide area network connecting local sites via public satellite channels only.

May/June 2007

**15.** Identify the incorrect statement regarding optical fiber cable from the options below.
(A) It transmits data as pulses of light rather than electrical pulses.
(B) The core is surrounded by glass cladding with a lower refraction index.
(C) It is utilized where massive amounts of data are sent on a regular basis.
(D) It is highly flexible and very simple to split and install.

Oct/Nov 2025

**16.** When transmitting digital data over enormous geographical distances utilizing existing analogue telephone voice channels, which technique is most appropriately employed?
(A) Transmission of digitally-modulated analogue carrier signals
(B) Direct-wire digital linking using unshielded twisted pair copper conductors
(C) Implementation of high-frequency unguided microwave signals
(D) Segregation of baseband digital pulses over dedicated coaxial cables

May/June 2012

**17.** Match the Guided Media cables (List I) with their structural characteristics (List II):
List I: (Guided Media Cables)
P. Twisted-pair
Q. Thin-net coaxial cable
R. Thick-net coaxial cable
S. Optical fiber cable
List II: (Structural Characteristics)
1. Uses BNC twist-on connectors and resembles television cables.
2. Consists of a glass core surrounded by glass cladding to keep light inside.
3. Rigid cable primarily used as a network backbone due to its larger diameter.
4. Uses strands of copper wire twisted together, commonly terminating in RJ-45 connectors.
(A) P-4, Q-1, R-3, S-2
(B) P-1, Q-2, R-4, S-3
(C) P-4, Q-3, R-1, S-2
(D) P-2, Q-4, R-3, S-1

Oct/Nov 2014

**18.** Consider the following statements regarding Wide Area Communication costs:
I Telephone companies charge a time/distance rate for a standard dial-up connection, regardless of the amount of information transmitted.
II Packet switching networks base their tariffs solely on the geographical distance between the two users.
Which of the above statement(s) is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

May/June 2019

**19.** Identify the incorrect pair from the following network concepts and their characteristics:
(A) Internet – Global network system available to all public users.
(B) Intranet – Exclusively available to users inside an organization.
(C) SLIP/PPP – Protocols used to establish dial-up for standalone PCs.
(D) Extranet – Grants anonymous users full access to the Intranet.

Oct/Nov 2006

**20.** A bank operates a WAN that connects its own branches. To facilitate a limited flow of data for clearing operations, it selectively links its network to the trusted networks of central regulatory and processing agencies. In the context of the bank's WAN, what term best describes these connected external networks?
(A) Extranet networks
(B) Local Area Networks
(C) Standalone Intranets
(D) Packet Switching Networks

May/June 2021

**21.** The following question consists of two statements—Assertion (A) and Reason (R).

NODIA

Answer the question by selecting the appropriate option.
Assertion (A): In microwave transmission, repeaters are needed periodically along the communication path.
Reason (R): Microwaves travel in a straight line, meaning the curvature of the earth will eventually get in the way if towers are too far apart.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2010**

**22.** Which of the following is an incorrect statement regarding the advantages of using Electronic Mail (E-mail)?
(A) Message delivery can be confirmed by the e-mail system.
(B) Both parties must be online simultaneously for delivery.
(C) Automated distribution to every member on a contact list.
(D) E-mail can effectively replace traditional telex terminals.

**May/June 2005**

**23.** Match the Internet Service Providers (List I) with their corresponding networks or services (List II) as available in India:
List I: (Internet Service Providers)
P. ERNET
Q. GIAS
R. NICNET
S. BSNL/MTNL
List II: (Networks or Services)
1. Gateway Internet Access Service
2. National Informatics Centre Network
3. Education & Research Network
4. PSTN terrestrial links for leased lines
(A) P-1, Q-3, R-4, S-2
(B) P-4, Q-2, R-1, S-3
(C) P-3, Q-4, R-2, S-1
(D) P-3, Q-1, R-2, S-4

**Oct/Nov 2022**

**24.** Consider the following statements regarding transmission media used in networking:
I Guided media confine signals to a narrow path so they behave predictably.
II Twisted-pair cables use twisting to reduce crosstalk between wires.
III Shielded twisted-pair cables feature a metal shield that grounds electromagnetic interference.
IV Unshielded twisted-pair cable is extremely rigid and primarily used as a network backbone.
V The RJ-45 connectors on twisted-pair cables resemble large telephone jacks.
Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (V)
(B) (I), (II), (IV), and (V)
(C) (II), (III), (IV), and (V)
(D) (I), (III), (IV), and (V)

**May/June 2018**

**25.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): Intranet utilizes Internet-derived communication protocols such as TCP/IP.
Reason (R): Intranet is technically identical to the Internet, except that access is restricted and not everybody is allowed to connect to it.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2016**

**26.** Research on the use of e-mail within organizations has demonstrated significant operational savings. What is the reported reduction in the amount of paper used?
(A) 95%
(B) 98%
(C) 80%
(D) 85%

NODIA

May/June 2014

**27.** What type of connectors are used specifically on coaxial cables in LAN environments?
(A) BNC twist-on connectors
(B) RJ-45 twist-on connectors
(C) RJ-11 snap-in connectors
(D) Fiber-optic ST connectors

Oct/Nov 2007

**28.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): For leased lines, the same rate is charged whether or not the communication facility is actively being used.
Reason (R): Leased lines are a dedicated link where the high performance is achieved because the line is permanently allocated by the telephone network.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2025

**29.** In the context of Local Area Network (LAN) hardware, interface hardware is required for any node to be connected to the physical network itself. By what technical term is this hardware commonly known?
(A) Modulator-Demodulator (Modem)
(B) Gateway Interface Switch (GIS)
(C) Network Interface Card (NIC) or Adapter
(D) Variable Length Subnet Mask (VLSM)

Oct/Nov 2019

**30.** Which of the following is NOT a requirement for establishing an on-line internet connection through a leased line?
(A) A hardware device with a configured IP address.
(B) An account on the service provider's system.
(C) A router for local network connectivity.
(D) A VSAT system with a personal earth station.

May/June 2009

**31.** Which networking device functions by dividing a single network up into separate smaller networks (or segments) to ensure that devices can communicate while mitigating throughput drops caused by data collisions?
(A) Repeater
(B) Concentrator
(C) Unmanaged Hub
(D) Bridge

Oct/Nov 2011

**32.** In determining the conceptual difference between Network-based IDS (NIDS) and Host-based IDS (HIDS), which of the following is accurate?
(A) NIDS relies on software agents, while HIDS is a standalone hardware unit.
(B) HIDS monitors host system files, while NIDS monitors network packets.
(C) NIDS is more expensive and requires more administration and training than HIDS.
(D) HIDS provides real-time detection globally across the entire network layout.

May/June 2010

**33.** A university campus needs to establish a central, high-speed physical path connecting the individual Local Area Networks of five different departmental buildings. Which of the following guided media components is primarily designed to serve as a network backbone in such a topology?
(A) Unshielded Twisted Pair (UTP)
(B) Thick-net Coaxial Cable
(C) RJ-45 Jumper Cables
(D) Thin-net Coaxial Cable

Oct/Nov 2024

**34.** Identify the incorrect statement regarding Remote Access Services.
(A) Dial-up remote access uses the public telephone network to create a physical connection to a remote access server port.
(B) A VPN creates an encrypted, virtual, point-to-point connection through the Internet.
(C) Using a VPN can reduce long distance phone expenses for companies by relying on existing internet infrastructure.
(D) Dial-up Remote Access Servers are often referred to synonymously as VPN Gateways.

Downloaded from www.pdf.tube

May/June 2017

**35.** Identify the incorrect statement regarding the differences between a Patch Panel and a Switch.
(A) A patch panel actively allocates resources and manages IP addressing for interconnected computers.
(B) A switch connects clients within a network to enable them to share data and access the internet.
(C) A patch panel in a LAN is a mounted hardware assembly containing ports to manage cables.
(D) A patch panel uses patch cords (jumper cables) to create and rearrange interconnections.

Oct/Nov 2005

**36.** Match the Remote Access mechanisms (List I) to their respective descriptions (List II):
List I: (Remote Access Mechanisms)
P. Dial-up Remote Access
Q. VPN Remote Access
R. RAS Server
S. RRAS
List II: (Descriptions)
1. A server that sits on the edge of the private network to accept physical telephone connections.
2. The software required to be installed to configure a server as a RAS/VPN server.
3. Uses an IP internetwork to create an encrypted, virtual connection.
4. Uses the public telephone network to create a direct physical connection.
(A) P-4, Q-3, R-1, S-2
(B) P-3, Q-4, R-2, S-1
(C) P-1, Q-2, R-3, S-4
(D) P-4, Q-1, R-3, S-2

May/June 2020

**37.** Which feature represents the most appropriate reason why twisted-pair wiring dominates modern business LANs over shielded alternatives?
(A) UTP cable is extremely inexpensive and highly flexible.
(B) It is immune to crosstalk without the need for twisting.
(C) It provides inherent protection against lightning strikes.
(D) It is the only media capable of transmitting at 10 Gbps.

Oct/Nov 2015

**38.** Which characteristic most appropriately defines Network Level Firewalls compared to Application Level Firewalls?
(A) Act solely as software proxies to filter web content.
(B) Run purely on open-source desktop operating systems.
(C) Designed specifically to allow unauthenticated logins.
(D) Utilize deep packet inspection on standalone hardware.

May/June 2013

**39.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): An Intrusion Prevention System (IPS) is considered an active prevention system, whereas an Intrusion Detection System (IDS) is a passive monitoring system.
Reason (R): An IDS is designed to inspect attack data and take corresponding action to block the attack before it succeeds.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Oct/Nov 2021

**40.** Match the networking devices (List I) with their primary operational role (List II):
List I: (Networking Devices)
P. Hub
Q. Switch
R. Router
S. Patch Panel
List II: (Primary Operational Role)
1. Acts as a dispatcher choosing the best route between multiple networks.
2. Performs no function except acting as a static connector for incoming/outgoing cables.
3. Connects cables together and merely regenerates data to pass from one device to another.
4. Serves as a controller to connect multiple

NODIA

devices on the same network and allows resource allocation.
(A) P-4, Q-3, R-2, S-1
(B) P-3, Q-1, R-4, S-2
(C) P-2, Q-4, R-1, S-3
(D) P-3, Q-4, R-1, S-2

**May/June 2024**

**41.** A financial institution wishes to allow its roaming consultants to securely access the central network using their standard Internet connections from hotels and cafes. They deploy a remote access solution running PPTP. Which technology are they actively utilizing?
(A) Dial-Up Remote Access Server
(B) Virtual Private Network (VPN) remote access
(C) Network-based Intrusion Detection System
(D) Point-to-Point physical telephony linkage

**Oct/Nov 2008**

**42.** Identify the correct pair connecting a transmission medium to its primary characteristic:
(A) Optical Fiber – Susceptible to high levels of interference.
(B) UTP Cable – Primarily utilizes BNC twist-on connector types.
(C) Coaxial Cable – Contains a single copper wire within a concentric channel.
(D) Guided Media – Signals transmitted via the open atmosphere.

**May/June 2006**

**43.** An organization wants to secure its internal network from unauthorized Internet users. It configures a device designed to execute an unauthenticated interactive login blockade. This device examines incoming messages and stops those that violate its rules. What is this device called?
(A) Hub
(B) Firewall
(C) Network Interface Card
(D) Patch Panel

**Oct/Nov 2017**

**44.** Which of the following networking components does NOT actively work to connect one computer to another by forwarding or routing digital data packets?
(A) Network Hub
(B) Router
(C) Network Switch
(D) Patch Panel

**May/June 2008**

**45.** The deployment of a Remote Access Service (RAS) involves several administrative and setup tasks. Which of the following is NOT one of the standard RAS setup and management tasks?
(A) Deciding what type of remote access users will need to use.
(B) Setting up the hardware for a dial-up remote access server.
(C) Configuring client operating systems for branch routers.
(D) Defining and setting specific remote access user permissions.

**Oct/Nov 2013**

**46.** Identify the correct statement related to LAN media.
(A) Optical fiber uses a metal shield to ground electromagnetic noise.
(B) The outer mesh or foil channel serves as an electrical ground.
(C) 10Base-FL and 100Base-FX refer to thick-net used by ISP networks.
(D) Unguided media confines signals to a specific manufactured path.

**May/June 2015**

**47.** Consider the following statements regarding network software:
I A Network Operating System (NOS) provides for either a Peer-to-Peer architecture or a Client/Server architecture.
II Device drivers are large software programs required for the router to operate with the firewall.
III Custom drivers for adapters must be copied into the NOS when the adapter is installed if they are not already included.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

**Oct/Nov 2012**

**48.** Consider the following functionalities:
I Connects multiple networks together to share an Internet connection.

Click Here to Buy book on Amazon

II Acts as a dispatcher, choosing the best route for information to travel.
III Analyzes data, changes how it is packaged, and sends it to a different type of network.
IV Connects multiple devices on the exact same network segment without analyzing external routes.

Which of the above functionalities describe the operation of a Router?
(A) (I), (II), and (III) only
(B) (I), (II), and (IV) only
(C) (II), (III), and (IV) only
(D) (I), (III), and (IV) only

**May/June 2011**

**49.** Network Level Firewalls typically run on proprietary operating systems. Which of the following operating systems is known to run on Cisco series network level firewalls?
(A) Cisco Internetwork Operating System
(B) Cisco Application Proxy Software
(C) Microsoft Windows Server RRAS
(D) Stateful Packet Inspection OS

**Oct/Nov 2020**

**50.** Consider the following statements about Firewalls:
I A firewall blocks unauthorized access while permitting authorized communications.
II Firewalls can be implemented strictly in hardware; software firewalls do not exist.
III All messages entering or leaving an intranet must pass through the firewall.
IV Network level firewalls are standalone boxes running proprietary operating systems like Cisco IOS.
V Application level firewalls offer content filtering and blocking of unwanted hosts.

Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (V)
(B) (I), (III), (IV), and (V)
(C) (II), (III), (IV), and (V)
(D) (I), (II), (IV), and (V)

**May/June 2022**

**51.** A company has a rapidly growing remote user population and its long distance telephone expenses are skyrocketing. Conceptually, why should the administrators consider shifting from Dial-Up Remote Access to a VPN Remote Access solution?
(A) VPN solutions use analogue ISDN adapters that eliminate the use of ISPs.
(B) VPN ensures all remote users stay strictly within the local calling area.
(C) Dial-Up Remote Access requires a dedicated expensive broadband connection.
(D) Employees can use local ISP dial-ins, avoiding long distance fees.

**Oct/Nov 2023**

**52.** Which of the following provides the conceptual distinction between a managed and an unmanaged switch?
(A) Managed switches work straight out of the box, while unmanaged must be programmed.
(B) Unmanaged switches operate at the Network Layer to connect multiple external networks.
(C) Managed switches allow configuration changes, while unmanaged do not.
(D) Managed switches are limited to home use, while unmanaged are used in datacenters.

**May/June 2016**

**53.** An enterprise needs to link its internal corporate network to an external network to share business applications. The required device must analyze data, protect the internal network from security threats, and route data across these distinctly different networks. Which device must the enterprise select?
(A) Concentrator
(B) Unmanaged Switch
(C) Router
(D) Patch Panel

**Oct/Nov 2009**

**54.** A bank's IT administrator suspects that a specific critical server is being targeted by a Trojan attempting to overwrite key system files. To monitor these specific local changes and halt the installation process, which security system is most appropriate to implement?
(A) Stateful Packet Inspection Firewall
(B) Network-based IDS (NIDS)
(C) Host-based IDS (HIDS)
(D) Unmanaged Switch

**May/June 2023**

**55.** Identify the correct statement concerning Intrusion Detection Systems (IDS).
(A) An IDS looks for known intrusion signatures

NODIA

or attack signatures that characterize different worms or viruses.
(B) An IDS prevents suspicious activity from taking place by actively blocking the traffic.
(C) A Host-based IDS (HIDS) utilizes hardware sensors located at various points along the external network boundary.
(D) A Network-based IDS (NIDS) can monitor activities that only an administrator should be able to implement on a single machine.

**Oct/Nov 2018**

**56.** Consider the following properties of radio waves:
I At low frequencies, radio waves pass through obstacles well, but power falls off sharply with distance.
II At high frequencies, radio waves tend to travel in straight lines and bounce off obstacles.
III Radio waves at high frequencies are completely immune to absorption by rain.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

**May/June 2007**

**57.** Which of the following correctly describes the setup requirement for Virtual Private Networking Servers?
(A) Installing one NIC connected to the company network and another NIC connected to the Internet via a dedicated line.
(B) Connecting a single network interface card (NIC) to both the internal network and the Internet simultaneously using a patch cord.
(C) Removing the Routing and Remote Access Services (RRAS) software from the ISP's gateway.
(D) Deploying an unmanaged switch to connect remote dial-up users directly to the corporate LAN without encryption.

**Oct/Nov 2025**

**58.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): A network bridge is often installed to connect separate network segments.
Reason (R): When more devices are connected to the same network, fewer collisions will happen, leading to an increase in average throughput.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2012**

**59.** The term "false positive" in the context of network security systems refers to which of the following?
(A) The system failing to detect a legitimate attack or security breach.
(B) The system allowing unauthorized users to modify host-based signatures.
(C) Incorrectly identifying legitimate requests as security breaches.
(D) The system's inability to update known intrusion signatures automatically.

**Oct/Nov 2014**

**60.** Consider the following statements regarding Virtual Private Networks (VPN) and IP phone networks:
I A Virtual Private Network allows remote employees to safely access the corporate network.
II An IP phone network separates a company's computer network from its telephone network to avoid unified communications.
Which of the above statement(s) is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**May/June 2019**

**61.** Conceptually, how does a communications satellite operate in a VSAT Network System?
(A) Functions as a data storage device holding internet caching data.
(B) Acts as a reflector, bouncing analog signals back using one frequency.
(C) Acts as a relay, retransmitting signals at different frequencies.
(D) Employs fiber optic cables in the atmosphere for zero-latency links.

Downloaded from www.pdf.tube

**Oct/Nov 2006**

**62.** Conceptually, how does a Software-Defined Wide Area Network (SD-WAN) improve upon the traditional router-centric strategy?
(A) Intelligently directs traffic to trusted SaaS and IaaS providers.
(B) Replaces all software routing with purely mechanical patch panels.
(C) Strictly confines data transmission to a single unshielded cable type.
(D) Operates in the presentation layer of the model to encrypt local data.

**May/June 2021**

**63.** Consider the following capabilities of ISDN channels:
I The Bearer (B) channel operates at 64 kbps and is used for voice, video, or data.
II B-channels cannot be aggregated together; they must remain isolated for bandwidth applications.
III The Delta (D) channel operates at either 16 kbps or 64 kbps.
IV The D-channel is primarily used for signaling communications between switching equipment.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (III)
(B) (I), (III), and (IV)
(C) (II), (III), and (IV)
(D) (I), (II), and (IV)

**Oct/Nov 2010**

**64.** Which of the following represents the most appropriate strategy for deploying wireless access points in a large corporate office to avoid signal degradation?
(A) Place one high-power access point next to the elevator shafts.
(B) Connect up to 100 users to one point to maximize hardware use.
(C) Space out access points and limit to 20 users per point.
(D) Install access points at the floor level rather than the ceiling.

**May/June 2005**

**65.** Technical requirements enable VSAT players to leverage modern SatCom technologies. Which of the following is NOT an emerging modern SatCom technology that allows VSAT players to leverage network capabilities?
(A) High Throughput Satellites (HTS)
(B) Non-Geostationary Orbit (NGSO) Satellites
(C) Sub-oceanic transponder relays
(D) Medium-earth orbit and low-earth orbit satellites

NODIA

**Oct/Nov 2022**

**66.** Identify the correct statement regarding WiMAX technology.
(A) Provides wide-area wireless data communication to multiple points.
(B) It stands for the Wireless Maximum Area Expansion architecture.
(C) Uses only licensed spectrum and is strictly for indoor deployments.
(D) Provides local access for a few hundred feet, topping at 54 Mbps.

**May/June 2018**

**67.** Consider the following statements about setting up Dial-up Remote Access Servers:
I If more than two modems are required in the pool, a multi-port serial adapter or a high-density combination card is used.
II A multi-port serial adapter allows the installation of a PCI or ISA card to create a large number of serial ports for modems.
Which of the above statement(s) is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**Oct/Nov 2016**

**68.** Most Indian banks migrated their domestic and international locations to a specific cloud technology due to its increased resiliency over traditional point-to-point (P2P) leased lines, despite it being considered pricey. Which technology is this?
(A) ISDN Basic Rate Interface
(B) MPLS cloud technology
(C) Unshielded Twisted Pair backbones
(D) Hub-and-Spoke Unmanaged Switching

**May/June 2014**

**69.** A network administrator wants to decrease latency, apply additional security, and easily control traffic patterns without physically moving devices. However, the administrator is warned that a single infected system may spread

a virus through the entire logical network. What architecture is being implemented?
(A) Virtual LAN (VLAN)
(B) Traditional thick-net bus topology
(C) Wide Area Network (WAN) Frame Relay
(D) Multi-port serial adapter pool

**Oct/Nov 2007**

**70.** A satellite receives a powerful transmitted signal from an earth station. To prevent this signal from interfering with the weak incoming signals, the satellite's transponder must perform which specific function?
(A) Convert the signal to a specific digital optical laser pulse.
(B) Store the signal and forward it after a set twenty-four-hour delay.
(C) Amplify and retransmit the signal at a different frequency.
(D) Broadcast the signal using the identical existing uplink frequency.

**May/June 2025**

**71.** Consider the following statements about Wi-Fi and WiMAX:
I Wi-Fi uses the 2.4 GHz, 3 GHz, 5 GHz, and 60 GHz radio frequency bands.
II WiMAX is designed to efficiently support from one to hundreds of CPEs.
III A single WiMAX antenna is expected to have a range of up to 40 miles.
IV Wi-Fi provides speeds up to 70 Mbps over distances of 40 miles.
V WiMAX can bring the underlying Internet connection needed to service local Wi-Fi networks.
Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (IV)
(B) (I), (II), (III), and (V)
(C) (II), (III), (IV), and (V)
(D) (I), (III), (IV), and (V)

**Oct/Nov 2019**

**72.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): Frame relay currently supports Switched Virtual Circuit (SVC), allowing connections to be changed easily.
Reason (R): ISDN requires all connections to be permanently nailed like frame relay.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2009**

**73.** Match the characteristics (List I) with the respective networking protocol/technology (List II):
List I: (Characteristics)
P. Operates at a layer considered "Layer 2.5"
Q. Spreads control across all network devices and simply directs traffic based on TCP/IP and ACLs
R. Enables intelligent application-aware routing
S. Removes latency in a network by allowing several networks to work virtually as one
List II: (Protocol/Technology)
1. VLAN
2. Traditional router-centric strategy
3. SD-WAN
4. MPLS
(A) P-3, Q-1, R-4, S-2
(B) P-4, Q-3, R-2, S-1
(C) P-2, Q-4, R-1, S-3
(D) P-4, Q-2, R-3, S-1

**Oct/Nov 2011**

**74.** Match the networking concepts (List I) to their respective features (List II):
List I: (Networking Concepts)
P. MPLS
Q. SD-WAN
R. VLAN
S. Traffic Engineering
List II: (Features)
1. A virtual WAN architecture that intelligently directs traffic to trusted SaaS and IaaS.
2. Allows several networks to work virtually as one LAN, decreasing latency.
3. The ability to set the path that the traffic will take through the network.
4. A data-carrying mechanism that integrates Layer 2 information into Layer 3.
(A) P-1, Q-2, R-3, S-4
(B) P-3, Q-4, R-1, S-2
(C) P-4, Q-1, R-2, S-3

Click Here to Buy book on Amazon

(D) P-4, Q-3, R-2, S-1

May/June 2010

**75.** Match the wireless networking concepts (List I) to their respective attributes (List II):

List I: (Wireless Networking Concepts)

P. Radio Frequency (RF)

Q. WiMAX

R. Wi-Fi

S. 3G and 4G connectivity

List II: (Attributes)

1. Expected to have a range of up to 40 miles with a speed of 70 Mbps or more.
2. Form of electromagnetic radiation with frequencies ranging from 3 Hz to 300 GHz.
3. Connectivity under GSM technology being actively considered for network designs.
4. Intended for LAN applications, scaling from one to tens of users with a 20 MHz channel size.

(A) P-1, Q-2, R-3, S-4
(B) P-2, Q-4, R-1, S-3
(C) P-3, Q-1, R-4, S-2
(D) P-2, Q-1, R-4, S-3

Oct/Nov 2024

**76.** Identify the incorrect statement regarding Integrated Services Digital Network (ISDN).

(A) It transports real-time voice, video, and non-real time LAN data.
(B) Setting up a connection is the same as making a regular phone call.
(C) ISDN charges are based on distance and time, similar to phone calls.
(D) An ISDN device can communicate directly with non-ISDN devices.

May/June 2017

**77.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.

Assertion (A): Wireless networks can cost less to operate than wired networks because they eliminate or reduce wiring costs.

Reason (R): The signal generated from each wireless access point weakens the longer it has to travel and can be negatively affected by metal and floors.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Oct/Nov 2005

**78.** What is the approximate geo-synchronous orbit distance above the earth for a communications satellite?

(A) 10,000 miles
(B) 15,000 miles
(C) 22,300 miles
(D) 36,000 miles

May/June 2020

**79.** Identify the correct statement detailing a key benefit of implementing Virtual LANs (VLANs).

(A) Physically wires all workstations into an immutable bus topology.
(B) Allows centralized configuration for separate geographical sites.
(C) Enforces severe latency to throttle heavy data bursts automatically.
(D) Entirely eliminates the risk of virus issues spreading via the network.

Oct/Nov 2015

**80.** Identify the incorrect statement regarding the benefits of VSAT networks for banks and financial institutions.

(A) They offer online connectivity for branches and standalone ATMs.
(B) They enable interactive distance learning for all branch staff members.
(C) They accommodate system expansion with very little increase in costs.
(D) They prohibit the two-way transmission of data and voice.

May/June 2013

**81.** Which of the following is NOT a security method explicitly recommended to consider for protecting a wireless network?

(A) Standard encryption of data transmitted over the air.
(B) Multi-factor user authentication for network access.
(C) Implementing a Token Ring directional token protocol.
(D) Control systems which protect mobile laptops and devices.

Downloaded from www.pdf.tube

Oct/Nov 2021

**82.** Which of the following most appropriately describes a capability of the ISDN Basic Rate Interface (BRI)?
(A) Combines channels into one faster connection as needed.
(B) Restricted to one voice conversation and cannot handle data.
(C) Supports exactly 23 B-channels for massive multimedia transfers.
(D) Replaces copper phone wires with a geo-synchronous satellite link.

May/June 2024

**83.** Identify the incorrect statement regarding the benefits of VSAT networks for banks and financial institutions.
(A) They offer online connectivity for branches and standalone ATMs.
(B) They enable interactive distance learning for all branch staff members.
(C) They accommodate system expansion with very little increase in costs.
(D) They prohibit the two-way transmission of data and voice.

Oct/Nov 2008

**84.** Which of the following is an incorrect statement regarding the disadvantages and limitations of VLANs?
(A) Risk of virus issues spreading through the whole logical network.
(B) VLANs are generally considered less efficient than a standard LAN.
(C) Requires patch cords to be unplugged when a workstation moves.
(D) VLANs are more effective at controlling latency than a typical WAN.

May/June 2006

**85.** In which year was the Internet Engineering Task Force's (IETF) Working Group formed for the technology that integrates Layer 2 data link information into Layer 3 network information?
(A) 1980
(B) 1993
(C) 1995
(D) 1997

Oct/Nov 2017

**86.** Match the ISDN configurations (List I) to their respective channel capacities (List II):
List I: (ISDN Configurations)
P. B-channel
Q. D-channel in BRI
R. Basic Rate Interface (BRI)
S. Primary Rate Interface (PRI)
List II: (Channel Capacities)
1. 23B+D channels over a high speed line
2. 64 kbps channel for voice, video, or data
3. 16 kbps channel for signaling
4. 2B+D channels over a standard phone line
(A) P-3, Q-2, R-1, S-4
(B) P-2, Q-3, R-4, S-1
(C) P-4, Q-1, R-3, S-2
(D) P-2, Q-4, R-3, S-1

May/June 2008

**87.** To support a Voice over Internet Protocol (VoIP) or Unified Communications system on a wireless network without potential degradation in voice quality, what is the maximum recommended number of users per access point?
(A) 1 to 5 users
(B) 8 to 12 users
(C) 20 to 30 users
(D) 50 to 100 users

NODIA

Oct/Nov 2013

**88.** Consider the following satellite communication bands and frequencies:
I C band: 6/4 GHz
II Ku band: 14/11 GHz
III Ka band: 30/20 GHz
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (I) and (III) only
(C) (II) and (III) only
(D) (I), (II), and (III)

May/June 2015

**89.** Consider the following characteristics regarding SD-WAN:
I It securely links users to applications using a mix of transport services like MPLS, LTE, and broadband.
II It relies on an outdated, rigid model that directs traffic strictly based on ACLs.
III It secures and intelligently directs traffic directly to trusted SaaS providers.
IV It lowers IT expenses while boosting corporate productivity and agility.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (III)
(B) (I), (III), and (IV)

(C) (II), (III), and (IV)
(D) (I), (II), and (IV)

**Oct/Nov 2012**

**90.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): Multiprotocol Label Switching (MPLS) directs data from one network node to the next based on long network IP addresses.
Reason (R): Label-based switching methods avoid complex lookups in a routing table by using simple labels.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2011**

**91.** In a particular network setup, a central hub has failed, immediately disabling all nodes attached to it, although no extra cable was required beyond what connects each node to the hub. Which physical topology does this describe?
(A) Linear Bus Topology
(B) Star Topology
(C) Ring Topology
(D) Full Mesh Topology

**Oct/Nov 2020**

**92.** To calculate the Network Address from a given IP address and a subnet mask, which specific bitwise mathematical operation is performed between them?
(A) Logical OR
(B) Logical XOR
(C) Logical AND
(D) Logical NAND

**May/June 2022**

**93.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): The OSI model has seven layers, whereas the TCP/IP model has four layers.
Reason (R): Some consider the TCP/IP model to have five layers, but when clubbing the bottom two layers ('physical' and 'network interface'), it is viewed as having four layers.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2023**

**94.** Which of the following most accurately contrasts the structural differences between IPv4 and IPv6 headers?
(A) IPv4 header is 40 bytes (8 fields); IPv6 is 20 bytes (13 fields).
(B) Headers are exactly 32 bytes, but IPv6 supports encryption natively.
(C) IPv4 header is 20 bytes (13 fields); IPv6 is 40 bytes (8 fields).
(D) IPv4 header is classless, while the IPv6 header uses classes A-E.

**May/June 2016**

**95.** Which of the following is NOT an advantage of the Ring network topology?
(A) Each node sends data when it receives an empty network token.
(B) Packets skip computers, making it faster than Star topology.
(C) It performs better than a Bus topology as the network load grows.
(D) There is no need for a central server to control the connectivity.

**Oct/Nov 2009**

**96.** Which of the following addresses represents the broadcast address that cannot be assigned to a host node in the subnet 200.133.175.16 (assuming a 4-bit subnet mask)?
(A) 200.133.175.17
(B) 200.133.175.30
(C) 200.133.175.31
(D) 200.133.175.32

**May/June 2023**

**97.** A software engineer is attempting to map the network communication models. When comparing the TCP/IP reference model to the

Click Here to Buy book on Amazon

OSI model, how does TCP/IP structure its top layer?
(A) Splits the Application layer into three distinct individual layers.
(B) Removes the Application layer, relying only on the Transport layer.
(C) Merges Application, Network, and Transport into one Protocol layer.
(D) Includes Session and Presentation within the Application layer.

**Oct/Nov 2018**

**98.** In what chronological sequence were the following Internet addressing and routing paradigms introduced?
(A) IPv6 → Classful IPv4 → Classless Inter-Domain Routing (CIDR)
(B) Classful IPv4 → Classless Inter-Domain Routing (CIDR) → IPv6
(C) Classless Inter-Domain Routing (CIDR) → Classful IPv4 → IPv6
(D) Classful IPv4 → IPv6 → Classless Inter-Domain Routing (CIDR)

**May/June 2007**

**99.** Which of the following is NOT a feature or characteristic of Classless Inter-Domain Routing (CIDR)?
(A) Introduced to address the lack of classful scalability.
(B) It is based on variable-length subnet masking.
(C) Enforces rigid Class A, B, and C boundaries for IPv4.
(D) Allows allocation based on arbitrary-length prefixes.

**Oct/Nov 2025**

**100.** An IT director is setting up a network where multiple star networks will be connected together to a central main bus. Which topology is the director implementing?
(A) Ring Topology
(B) Point-to-Point Topology
(C) Tree Topology
(D) Mesh Topology

**May/June 2012**

**101.** Which of the following represents the most appropriate explanation for why IPv6 design resulted in slower growth of routing tables in internet routers?
(A) It allows more efficient aggregation of subnetwork prefixes.
(B) It forced all ISPs to drop IPv4 connectivity simultaneously.
(C) It eliminated the need for built-in strong security features.
(D) It restricted individual allocations to a maximum of 256 hosts.

**Oct/Nov 2014**

**102.** Identify the incorrect statement regarding the Ring network topology.
(A) There is a central computer or server to which all the workstations are directly connected to control connectivity.
(B) The workstations are connected in a closed loop configuration.
(C) If a Token Ring protocol is used, the signal travels in only one direction.
(D) Each packet of data must pass through all the computers between source and destination, making it slower than Star topology.

**May/June 2019**

**103.** Match the IP Address Class (List I) to its default Subnet Mask (List II):
List I: (IP Address Class)
P. Class A
Q. Class B
R. Class C
S. Class D
List II: (Default Subnet Mask)
1. 255.255.0.0
2. 255.0.0.0
3. Not equipped with any subnet masking
4. 255.255.255.0
(A) P-1, Q-2, R-3, S-4
(B) P-2, Q-1, R-4, S-3
(C) P-2, Q-4, R-1, S-3
(D) P-4, Q-1, R-2, S-3

NODIA

**Oct/Nov 2006**

**104.** Match the IPv4 Address Classes (List I) to their respective Address Ranges (List II):
List I: (IPv4 Address Classes)
P. Class A
Q. Class B
R. Class C
S. Class D
List II: (Address Ranges)
1. 192.0.1.1 to 223.255.254.254
2. 224.0.0.0 to 239.255.255.255

3. 1.0.0.1 to 126.255.255.254
4. 128.1.0.1 to 191.255.255.254

(A) P-4, Q-3, R-2, S-1
(B) P-3, Q-1, R-4, S-2
(C) P-1, Q-2, R-3, S-4
(D) P-3, Q-4, R-1, S-2

**May/June 2021**

**105.** Match the IP protocol version (List I) with its specific characteristics (List II):

List I: (IP Protocol Version)
P. IPv4
Q. IPv6
R. IPv4 Header
S. IPv6 Address representation

List II: (Characteristics)
1. Contains 13 fields and is 20 bytes long
2. Uses a prefix and an Identifier ID instead of a subnet mask
3. Subdivided into classes A, B, C, D, E
4. 128 bits in size

(A) P-1, Q-4, R-3, S-2
(B) P-3, Q-1, R-2, S-4
(C) P-3, Q-2, R-1, S-4
(D) P-2, Q-3, R-4, S-1

**Oct/Nov 2010**

**106.** Conceptually, which protocol within the TCP/IP stack provides a discrete packet delivery service for applications, like a messaging service, without any guarantee of delivery?

(A) Internet Protocol (IP)
(B) User Datagram Protocol (UDP)
(C) Transmission Control Protocol (TCP)
(D) Post Office Protocol (POP)

**May/June 2005**

**107.** Which feature represents the most appropriate justification for why IPv6 is deemed sufficient for the foreseeable future regarding address space?

(A) Increases address size to 128 bits, providing $3.4 \times 10^{38}$ IPs.
(B) Increases address size to 64 bits, providing $4.3 \times 10^{9}$ IPs.
(C) Introduces a 20-byte header that dynamically creates new classes.
(D) Forces all users onto one subnet mask, unlocking unlimited nodes.

**Oct/Nov 2022**

**108.** Consider the following statements regarding the Mesh network topology:

I In a full mesh topology, each workstation is connected directly to each of the others.
II A broken node will distract the transmission of data and bring the entire mesh network down.
III A mesh topology can handle a high amount of network traffic since every additional device is considered a node.
IV Building this topology requires a lot of capital to invest in due to the vast number of devices and connections needed.

Which of the above statement(s) is/are correct?

(A) (I), (II), and (III)
(B) (I), (III), and (IV)
(C) (II), (III), and (IV)
(D) (I), (II), and (IV)

**May/June 2018**

**109.** Identify the correct statement regarding restrictions on subnet addresses.

(A) Node addresses consisting of all "1"s are reserved for multicasting.
(B) A 1-bit subnet mask is permitted on all modern legacy devices without restriction.
(C) The formula for calculating the number of subnets is simply $2^n$ without any subtractions.
(D) Node addresses consisting of all "0"s are reserved for specifying the local network address.

**Oct/Nov 2016**

**110.** A network engineer is reviewing an IPv4 address `140.179.220.200`. Which of the following accurately identifies the default Network part and Node part for this address?

(A) It is a Class A address; Network part is `140.x.x.x`, Node part is `x.179.220.200`.
(B) It is a Class C address; Network part is `140.179.220.x`, Node part is `x.x.x.200`.
(C) It is a Class B address; Network part is `140.179.x.x`, Node part is `x.x.220.200`.
(D) It is a Class D address reserved for multicasting.

**May/June 2014**

**111.** Consider the following reasons for subnetting an IP Network:

I Organization of different physical media

Downloaded from www.pdf.tube

(Ethernet, FDDI, WAN).
II Preservation of address space.
III Implementation of security measures.
IV Minimizing network traffic by limiting the packets nodes on a segment receive.
V Converting IPv4 32-bit addresses into IPv6 128-bit addresses dynamically.
Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (V)
(B) (I), (II), (III), and (IV)
(C) (II), (III), (IV), and (V)
(D) (I), (III), (IV), and (V)

**Oct/Nov 2007**

**112.** When an application on a host computer sends a request to another application on a different host, in what chronological order does the packet travel through the model layers on the originating computer?
(A) Physical → Data Link → Network → Transport → Application
(B) Application → lower layer adding header/footer → physical layer → transmitted through cable
(C) Physical layer → reading/deciphering header → removing footer → Application
(D) Network → Transport → Application → Physical

**May/June 2025**

**113.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): In a star topology, it is easy to detect faults and to remove parts without disrupting the network when connecting or removing devices.
Reason (R): Every workstation is directly connected to every other workstation through a closed loop configuration.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2019**

**114.** An organization is assigned a Class C network number of 200.133.175.0. The administrator wants to break this network into 14 subnets of 14 nodes each. To accomplish this, how many bits long must the subnet mask extension be?
(A) 2 bits
(B) 3 bits
(C) 4 bits
(D) 5 bits

**May/June 2009**

**115.** A small office is setting up an internal LAN behind a Network Address Translator (NAT). They must choose an IP address range that routers on the Internet will never forward. Which of the following is a valid private subnet address block they can use?
(A) 11.0.0.0/8
(B) 192.169.0.0/16
(C) 126.255.255.0/24
(D) 172.16.0.0/12

NODIA

**Oct/Nov 2011**

**116.** Consider the following statements regarding network topology definitions:
I Physical topology refers to the actual geometric layout of workstations.
II Logical (or signal) topology refers to the nature of the paths the signals follow from node to node.
Which of the above statement(s) is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**May/June 2010**

**117.** A network engineer is working with an IP address and applying a 3-bit subnet mask. According to the formula $(2^n - 2)$, how many available subnets does this size mask produce?
(A) 4 subnets
(B) 6 subnets
(C) 8 subnets
(D) 14 subnets

**Oct/Nov 2024**

**118.** Identify the correct statement regarding network topologies.
(A) A Star topology requires less cable length than a linear bus topology.
(B) In a partial mesh topology, every single

workstation is connected directly to every other workstation.
(C) The tree network topology uses two or more ring networks connected to a central hub.
(D) A Linear Bus topology requires terminators at both ends of the backbone cable.

**May/June 2017**

**119.** Identify the incorrect statement regarding subnetting calculations.
(A) A 3-bit subnet mask provides exactly 8 available subnets for use in legacy environments.
(B) The "–2" in the formula accounts for the network address and the broadcast address which cannot be assigned to host nodes.
(C) The formula to calculate the number of available subnets or nodes is $(2^n - 2)$, where $n$ equals the number of bits.
(D) Subnetting minimizes the amount of traffic each segment must receive by controlling collisions.

**Oct/Nov 2005**

**120.** Consider the following statements regarding IP addressing:
I An IPv4 address is a 32-bit binary number represented as 4 decimal values.
II Addresses beginning with 127 decimal are reserved for loopback and internal testing.
III IPv6 addresses are 128 bits in size and usually represented with eight hexadecimal groups.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

**May/June 2020**

**121.** Which of the following best represents the chronological evolution of IP addressing strategies as the Internet expanded?
(A) IPv6 adoption → Introduction of VLSM → Classful Network Design
(B) Classless Inter-Domain Routing (CIDR) → IPv6 deployment → Classful address exhaustion
(C) Classful network design → Classless Inter-Domain Routing (CIDR) → IPv6 deployment
(D) Variable-Length Subnet Masking (VLSM) → Class A/B/C addressing → IPv4

**Oct/Nov 2015**

**122.** Identify the correct statement regarding the security features embedded within the Internet Protocol versions.
(A) IPv4 comes with mandatory security including packet inspection.
(B) IPv4 inherently enforces IPsec over all transmission links.
(C) IPv6 supports native encryption and authentication features.
(D) IPv6 encryption and authentication are rarely supported today.

**May/June 2013**

**123.** Identify the incorrect statement regarding the application of a subnet mask.
(A) The network bits are represented by 1s in the mask, and the node bits are represented by 0s.
(B) Additional bits can be added to the default subnet mask for a given Class to break down a network further.
(C) The term subnet mask is used exclusively within IPv6 routing protocols.
(D) Performing a bitwise logical AND operation between the IP address and the subnet mask results in the Network Address.

**Oct/Nov 2021**

**124.** Consider the following statements regarding the TCP/IP stack layers and protocols:
I IP provides a common address space and routes packets across the entire internet.
II TCP provides discrete, guaranteed, extremely reliable data transmission.
III UDP provides a discrete packet delivery service without a guarantee of delivery.
IV The physical and network interface layers are sometimes clubbed as a single 'host to network' layer.
V The TCP/IP model entirely separates the session and presentation layers from the application layer.
Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (V)
(B) (I), (II), (III), and (IV)
(C) (II), (III), (IV), and (V)
(D) (I), (III), (IV), and (V)

Click Here to Buy book on Amazon

**May/June 2024**

**125.** Which of the following is NOT an IP network address reserved exclusively for private networks?

(A) 10.0.0.0/8

(B) 224.0.0.0/4

(C) 172.16.0.0/12

(D) 192.168.0.0/16

www.nodia.in

NODIA

# ANSWERS

1. (D) A dedicated physical firewall appliance
E-mail systems require computers at both ends, communication devices like modems to convert signals, and specialized software to manage message transmission. While firewalls provide security, a dedicated physical appliance is not a fundamental functional requirement for the communication link itself. The system relies primarily on software protocols and basic hardware connectivity for data flow.

2. (C) On-line connectivity provides flat-fee dedicated Internet access.
On-line connectivity implies a permanent, dedicated link typically provided via leased lines or broadband, usually involving a flat fee regardless of usage duration. Conversely, off-line or dial-up connections are temporary, established only when needed, and often billed based on the time spent connected. This distinction centers on the availability and cost structure of the access.

3. (C) It offers high performance because the line is permanently allocated by the telephone network.
Leased lines provide a dedicated, private communication path between two points that remains active at all times. Because the telephone network allocates the bandwidth exclusively to the subscriber, it ensures high performance and consistent reliability. This permanent nature means the user is charged a fixed rate regardless of the actual data volume or time spent transmitting.

4. (C) Optical Fiber Cable
Optical fiber transmits data using light pulses through glass strands, making it entirely immune to electromagnetic interference generated by heavy machinery. It supports extremely high bandwidth and can carry signals over very long distances without significant degradation. This makes it superior to copper-based cables like UTP or coaxial in environments with high electrical noise.

5. (A) (I) and (II) only
Terrestrial links for internet connectivity frequently utilize public switched telephone or data networks for wired access. Wireless wide area connectivity is commonly achieved through satellite systems. In India, private organizations are permitted to provide internet and e-mail services, making the third statement incorrect. Therefore, only the descriptions of wired and wireless connectivity methods are accurate.

6. (B) Radio waves penetrate buildings, whereas microwaves travel in straight lines.
Radio waves at lower frequencies can penetrate obstacles like walls and buildings, facilitating broad coverage. In contrast, microwaves operate at higher frequencies and travel strictly in line-of-sight paths, requiring precisely aligned antennas. While radio waves are omni-directional, microwaves behave more like light and are easily blocked or reflected by physical structures in their path.

7. (B) A store and forward basis utilizing a mailbox located in a computer
Electronic mail functions using a store and forward mechanism where messages are sent to a server and held in a digital mailbox. The recipient does not need to be online to receive the data immediately. Instead, the server stores the message until the user connects and retrieves it, allowing for asynchronous communication across different networks.

8. (B) Broadband connections typically offer speeds of 700 kbit/s or higher.
Broadband technology provides high-speed internet access that is significantly faster than traditional dial-up services, often exceeding several hundred kilobits per second. Unlike dial-up, broadband is an always-on connection that does not require an exclusive phone line, allowing users to browse and use telephony simultaneously. This shift has redefined global digital connectivity standards and user experiences.

NODIA

**9.** (B) The network utilizes a widely dispersed, non-shared public transmission medium.
Local Area Networks are confined to limited geographic areas like single buildings and use shared, private transmission media rather than public ones. They are characterized by high data transfer rates and peer-to-peer device interactions. Using a widely dispersed public medium is a feature of Wide Area Networks, which connect geographically remote sites across cities or countries.

**10.** (C) The slow speed of the dial-up line directly inflates the time-based call charges.
Dial-up connections are billed based on the duration of the telephone call. Because dial-up has relatively low data transfer speeds, sending large volumes of data takes a significant amount of time. Consequently, the accumulated time-based charges for a single large transfer can quickly exceed the fixed costs associated with faster, dedicated alternatives like leased lines.

**11.** (A) Only (I)
Thick-net coaxial cable is thicker and less flexible than thin-net, but its size allows it to transmit signals over longer distances without significant loss. While thin-net is easier to install for individual workstations, it is not used as a backbone; rather, thick-net typically serves as the main network backbone due to its superior range and durability.

**12.** (C) A Packet Switching Network (PSN)
Packet Switching Networks are generally the most cost-effective choice for transferring mid-volume data between remote locations because they charge based on the amount of information sent. Unlike leased lines, which have high fixed costs, or dial-up, which has high time-based costs, PSNs allow multiple users to share resources, optimizing expenses for moderate data traffic requirements.

**13.** (C) (I), (II), and (IV) only
Intranets utilize internet technologies like web browsers to manage distributed corporate information and integrate various business processes. They help streamline human resources, finance, and supply chain management across an organization. Since they support standard web protocols, claiming they are limited only to email is incorrect. They are vital for enhancing internal communication and productivity in modern digital economies.

**14.** (C) A closed network using internet technology to manage corporate data.
An Intranet is a private, restricted network that employs the same protocols and software as the public Internet but is accessible only to members of a specific organization. It serves as a secure platform for sharing internal data, collaborating on projects, and managing corporate resources. Unlike the global Internet, it is closed off from unauthorized external access.

**15.** (D) It is highly flexible and very simple to split and install.
Optical fiber cable is constructed with a glass core that transmits data as light pulses, offering high capacity for massive data transfers. However, it is not simple to split or install compared to copper wiring. The glass material is fragile, requires specialized tools for splicing, and must not be bent sharply, making its deployment complex and demanding.

**16.** (A) Transmission of digitally-modulated analogue carrier signals
Existing telephone lines are designed for analog voice signals. To send digital data over these channels across long distances, the digital pulses must be converted into analog waves through modulation. A modem performs this task, allowing digital information to travel as modulated carrier signals that the recipient's modem then demodulates back into the original digital format.

**17.** (A) P-4, Q-1, R-3, S-2
Twisted-pair cabling consists of copper strands often ending in RJ-45 connectors. Thin-net coaxial resembles television cable using BNC connectors, while thick-net is a rigid backbone medium. Optical fiber uses glass cores and cladding to transmit light. Matching these characteristics involves identifying the specific physical construction and connector types associated with each common type of guided network media.

Downloaded from www.pdf.tube

**18.** (A) Only (I)
For standard dial-up connections, telephone companies typically charge based on the duration and distance of the call, irrespective of the data volume. In contrast, packet switching networks usually base their tariffs on the amount of data transmitted rather than the geographical distance. Therefore, the first statement accurately reflects dial-up billing, while the second misrepresents packet switching.

**19.** (D) Extranet – Grants anonymous users full access to the Intranet.
An Extranet is an extension of an Intranet that allows specific, authorized external users, such as partners or customers, to access limited internal resources. It does not provide full or anonymous access to the entire Intranet. Access remains strictly controlled through authentication to ensure that only trusted parties can interact with the organization's private data and systems.

**20.** (A) Extranet networks
When a private network like a bank's WAN is selectively connected to external, trusted networks for specific operations, it creates an Extranet. This setup allows controlled communication and data exchange with authorized outside entities, such as regulatory agencies, while maintaining overall security. It facilitates business-to-business interactions without exposing the entire internal network to the general public internet.

**21.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Microwaves travel in straight lines, which limits their range to the visual horizon. Because the earth is curved, the signal will eventually be blocked if the towers are placed too far apart. To overcome this physical limitation and maintain a communication link over long distances, repeaters must be installed periodically to catch, amplify, and retransmit the signal.

**22.** (B) Both parties must be online simultaneously for delivery.
One of the primary advantages of electronic mail is that it operates as an asynchronous communication tool. The sender and recipient do not need to be online at the same time. Messages are stored on a server until the recipient retrieves them. This flexibility distinguishes e-mail from real-time communication methods like phone calls or certain instant messaging services.

**23.** (D) P-3, Q-1, R-2, S-4
In the Indian context, ERNET is dedicated to education and research, while GIAS stands for Gateway Internet Access Service. NICNET is the network managed by the National Informatics Centre. BSNL and MTNL provide terrestrial links using the public switched telephone network. Correctly matching these entities requires identifying their specific roles and the network services they traditionally offer.

**24.** (A) (I), (II), (III), and (V)
Guided media like twisted-pair and coaxial cables confine signals to a specific path, ensuring predictable behavior. Twisting wires reduces crosstalk, and shielding protects against electromagnetic interference. RJ-45 connectors are the standard for these cables. The statement that unshielded twisted-pair is rigid and used as a backbone is incorrect, as it is actually flexible and used for workstation connections.

**25.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Intranets are technically designed using the same foundational protocols as the Internet, such as TCP/IP, and use similar software like web browsers. The fundamental difference lies in access control; an Intranet is a private network where access is restricted to authorized users within an organization. This shared technical basis allows for easy integration of standard internet-based tools.

**26.** (D) 85%
Organizational research has highlighted that the adoption of electronic mail systems significantly reduces the reliance on physical documentation. By enabling digital messaging and file sharing, e-mail has been shown to decrease the amount of paper used within corporate environments by approximately eighty-five percent. This shift contributes to both operational cost savings and improved environmental sustainability for modern businesses.

NODIA

**27.** (A) BNC twist-on connectors
In Local Area Network environments using coaxial cabling, BNC connectors are the standard hardware for establishing connections. These are twist-on connectors that secure the cable to network interface cards or other devices. Unlike RJ-45 connectors, which are used for twisted-pair wiring, BNC connectors are specifically designed to maintain the integrity of the signal within a coaxial structure.

**28.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Leased lines involve a permanent allocation of network resources by the telephone company, ensuring high performance for the subscriber. Because this link is dedicated exclusively to the user at all times, the billing is based on a fixed rate. This cost remains constant regardless of whether the line is being actively used to transmit data or is sitting idle.

**29.** (C) Network Interface Card (NIC) or Adapter
Every node on a Local Area Network requires specific interface hardware to connect to the physical transmission medium. This device, commonly known as a Network Interface Card or adapter, manages the flow of data between the computer and the network cable. It provides the physical port and the necessary electronics to translate internal data into signals for transmission.

**30.** (D) A VSAT system with a personal earth station.
Establishing an on-line internet connection via a leased line requires a configured IP address, a provider account, and a router to manage local traffic. However, a VSAT system is a completely different technology that uses satellite communication rather than terrestrial leased lines. Therefore, a personal earth station is not a requirement for a standard terrestrial leased line setup.

**31.** (D) Bridge
A bridge is a networking device used to divide a large network into smaller segments. By filtering traffic based on hardware addresses, it ensures that local communication stays within its segment while only necessary data crosses over. This reduction in the number of devices per segment helps mitigate data collisions and prevents throughput drops, improving overall network efficiency.

**32.** (B) HIDS monitors host system files, while NIDS monitors network packets.
Host-based Intrusion Detection Systems (HIDS) are installed on individual machines to monitor local activities, such as changes to system files or registry entries. In contrast, Network-based Intrusion Detection Systems (NIDS) analyze traffic flowing across the network to identify suspicious patterns or signatures. Each type provides a different layer of security, targeting either local host integrity or network-wide traffic.

**33.** (B) Thick-net Coaxial Cable
Thick-net coaxial cable is historically designed to serve as a network backbone due to its ability to carry signals over longer distances without significant loss. It is more rigid and durable than thin-net or standard UTP cables. In a campus environment, it provides the main high-speed path that interconnects different departmental buildings, forming the core of the network topology.

**34.** (D) Dial-up Remote Access Servers are often referred to synonymously as VPN Gateways.
Dial-up remote access creates a physical connection over the public telephone network, whereas a Virtual Private Network (VPN) creates an encrypted, virtual tunnel over the Internet. Because these technologies operate differently and use different infrastructures, their server components are not synonymous. A VPN gateway manages internet-based tunnels, while a dial-up server manages physical modem banks and telephone lines.

**35.** (A) A patch panel actively allocates resources and manages IP addressing for interconnected computers.
A patch panel is a passive hardware assembly used for organizing and managing cable interconnections in a network rack. It does not possess the intelligence to allocate resources or manage IP addresses. Those active functions are performed by switches or routers. The primary role of a patch panel is simply to provide a static location to terminate and rearrange wiring.

Click Here to Buy book on Amazon

**36.** (A) P-4, Q-3, R-1, S-2
Dial-up access uses the telephone network for physical links, while VPNs create encrypted virtual connections over IP networks. A Remote Access Server (RAS) sits at the network edge to accept these connections. Routing and Remote Access Service (RRAS) is the software used to configure such servers. Matching these terms involves distinguishing between the connection types and their hardware/software components.

**37.** (A) UTP cable is extremely inexpensive and highly flexible.
Unshielded Twisted Pair (UTP) cabling is the most common choice for modern business LANs because it is cost-effective and easy to install. Its flexibility allows it to be pulled through conduits and around corners more easily than rigid coaxial cables. While it lacks the shielding of other media, its performance and low cost make it ideal for most office environments.

**38.** (D) Utilize deep packet inspection on standalone hardware.
Network-level firewalls are typically dedicated hardware appliances that perform deep packet inspection to filter traffic based on IP addresses and ports. They often run proprietary operating systems designed for high-speed security processing. Unlike application-level firewalls, which act as proxies for specific programs, network firewalls operate at lower layers of the stack to protect the entire network perimeter from unauthorized access.

**39.** (C) Assertion (A) is true, but Reason (R) is false.
An Intrusion Prevention System (IPS) is active because it can block traffic in real-time when an attack is detected. An Intrusion Detection System (IDS) is passive, as its primary role is to monitor and alert administrators rather than take direct action to stop the threat. The claim that an IDS is designed to block attacks before they succeed is incorrect.

**40.** (D) P-3, Q-4, R-1, S-2
A hub simply regenerates data across all ports, while a switch intelligently connects devices on the same network and allocates resources. A router acts as a dispatcher to move data between different networks. A patch panel is a static hardware assembly for cable management. Matching these roles requires understanding how each device processes and directs data within a network.

**41.** (B) Virtual Private Network (VPN) remote access
Roaming users who need secure access to a central network via their own internet connections typically utilize Virtual Private Network (VPN) technology. By using protocols like PPTP, a VPN creates an encrypted tunnel over the public internet, ensuring that sensitive data remains protected. This allows employees to work securely from various locations without needing dedicated point-to-point physical telephone links.

**42.** (C) Coaxial Cable – Contains a single copper wire within a concentric channel.
Coaxial cable is designed with a single central copper conductor surrounded by an insulating layer and a grounded metal shield, all contained within a concentric channel. Optical fiber is immune to interference, unlike copper. UTP cables typically use RJ-45 connectors, not BNC. Guided media involves physical paths like cables, whereas signals in the open atmosphere are characteristic of unguided media.

NODIA

**43.** (B) Firewall
A firewall is a security device or software that monitors and controls incoming and outgoing network traffic based on predetermined rules. It serves as a barrier between a trusted internal network and untrusted external networks like the Internet. By blocking unauthorized interactive logins and stopping messages that violate security policies, it protects the internal system from various cyber threats and intrusions.

**44.** (D) Patch Panel
Hubs, routers, and switches are active networking devices that process, forward, or route digital data packets to connect computers. In contrast, a patch panel is a passive hardware component used solely for organizing and terminating network cables. It does not have the electronic circuitry required to analyze or direct data traffic; it merely provides a convenient place for physical interconnections.

**45.** (C) Configuring client operating systems for branch routers.
Setting up a Remote Access Service (RAS) involves determining user needs, configuring the server hardware and software, and defining specific user permissions. While client computers must be configured to connect to the RAS, configuring branch routers is generally considered a separate network infrastructure task. RAS management focuses on the gateway that allows individual remote users to access the private network.

**46.** (B) The outer mesh or foil channel serves as an electrical ground.
In shielded cables like coaxial or shielded twisted pair, an outer metal mesh or foil layer serves as an electrical ground to protect the signal from external interference. Optical fiber does not use metal shields as it transmits light. 10Base-FL and 100Base-FX are fiber optic standards, not thick-net. Unguided media transmits through the air, whereas guided media uses cables.

**47.** (C) (I) and (III) only
A Network Operating System (NOS) supports either peer-to-peer or client/server architectures. For network adapters to function, custom device drivers must be present in the NOS. Device drivers are typically small, specialized programs rather than large ones, and they facilitate communication between the hardware and the operating system rather than specifically between a router and a firewall.

**48.** (A) (I), (II), and (III) only
Routers connect different networks, act as dispatchers to find the best data paths, and can translate data between different network types. They operate by analyzing network addresses to route traffic externally. Connecting devices on the exact same network segment without analyzing external routes is a function of a switch or a hub, rather than a primary characteristic of a router.

**49.** (A) Cisco Internetwork Operating System
Cisco series network-level firewalls typically run on the Cisco Internetwork Operating System (IOS), which is a proprietary operating system designed for networking equipment. This OS provides the necessary tools for routing, switching, and implementing robust security features like stateful packet inspection. It is distinct from general-purpose desktop operating systems and is optimized for the hardware it controls in a network.

**50.** (B) (I), (III), (IV), and (V)
Firewalls control access by filtering communications according to set rules, and all traffic entering or leaving the protected network must pass through them. They can be implemented in both hardware and software. Network-level firewalls often use proprietary operating systems like Cisco IOS, while application-level firewalls provide specific content filtering. These components together ensure a comprehensive security perimeter for organizations.

**51.** (D) Employees can use local ISP dial-ins, avoiding long distance fees.
Shifting from dial-up to a VPN allows remote employees to connect to a local Internet Service Provider instead of making a direct, long-distance call to the company's server. Once online, they use the VPN to create a secure, encrypted tunnel to the office. This strategy leverages existing internet infrastructure to significantly reduce expensive long-distance telephone charges for the organization.

**52.** (C) Managed switches allow configuration changes, while unmanaged do not.
An unmanaged switch is a plug-and-play device that works with a fixed configuration and cannot be modified. In contrast, a managed switch allows administrators to adjust settings, such as prioritizing traffic, creating VLANs, and monitoring performance. This flexibility makes managed switches suitable for complex corporate networks where fine-grained control over data flow and security is required for operational efficiency.

**53.** (C) Router
A router is the essential device for linking an internal corporate network to an external one because it can analyze data packets and determine the best path across different networks. It also provides a level of security by filtering traffic and can handle the translation needed between distinct network architectures. This makes it far more capable than simple switches or patch panels.

Downloaded from www.pdf.tube

**54.** (C) Host-based IDS (HIDS)
A Host-based Intrusion Detection System (HIDS) is designed to monitor the activity on a specific server or computer. It tracks changes to critical system files, registry entries, and local logs to detect unauthorized modifications, such as those caused by a Trojan. Because it operates within the host operating system, it can identify and halt malicious processes that network-based systems might miss.

**55.** (A) An IDS looks for known intrusion signatures or attack signatures that characterize different worms or viruses.
An Intrusion Detection System (IDS) works by comparing network traffic or system activity against a database of known attack signatures, which are patterns associated with specific threats like worms or viruses. While an IPS can block traffic, a traditional IDS is primarily used for monitoring and alerting. HIDS focuses on local host systems, while NIDS monitors traffic across the entire network.

**56.** (A) (I) and (II) only
At low frequencies, radio waves can pass through obstacles easily but lose power quickly as the distance increases. At higher frequencies, they tend to travel in straight lines and can reflect off surfaces. High-frequency radio waves are not immune to rain; in fact, they are susceptible to absorption by atmospheric moisture, which can degrade the signal strength over long distances.

**57.** (A) Installing one NIC connected to the company network and another NIC connected to the Internet via a dedicated line.
Setting up a Virtual Private Networking (VPN) server typically requires two network interface cards (NICs). One card connects the server to the internal private corporate network, while the second card connects to the public Internet through a dedicated line or gateway. This dual-homed configuration allows the server to act as a secure bridge, encrypting and routing traffic between the two networks.

**58.** (C) Assertion (A) is true, but Reason (R) is false.
A network bridge is indeed used to connect separate segments and improve efficiency. However, the reasoning provided is incorrect; adding more devices to the same network segment actually increases the likelihood of data collisions. Bridges help by dividing the network into smaller collision domains, which reduces the number of devices per segment and thereby increases the overall average throughput.

**59.** (C) Incorrectly identifying legitimate requests as security breaches.
In network security, a false positive occurs when an Intrusion Detection System or firewall incorrectly flags normal, legitimate activity as a potential threat or attack. This can lead to unnecessary alerts for administrators and might even cause legitimate traffic to be blocked if an automated prevention system is in place. Minimizing false positives is crucial for maintaining efficient and reliable network operations.

**60.** (A) Only (I)
A Virtual Private Network (VPN) provides remote employees with secure access to their company's internal network over the public internet. Conversely, an IP phone network is often integrated with the computer network to enable unified communications, such as voice and data sharing, rather than being strictly separated to avoid it. Therefore, only the first statement regarding the function of VPNs is correct.

**61.** (C) Acts as a relay, retransmitting signals at different frequencies.
In a VSAT network, a communications satellite serves as a relay station in space. It receives signals transmitted from an earth station, amplifies them, and then retransmits them back to other earth stations. To avoid interference between the powerful uplink and the weaker downlink, the satellite typically uses different frequencies for receiving and sending the data, facilitating reliable wide-area communication.

**62.** (A) Intelligently directs traffic to trusted SaaS and IaaS providers.
A Software-Defined Wide Area Network (SD-WAN) improves upon traditional router-centric models by using software to intelligently manage and direct traffic across the WAN. It can prioritize critical applications and securely route data directly to trusted cloud services like SaaS and IaaS. This approach increases network agility, improves application performance, and reduces

NODIA

costs compared to rigid, manually configured hardware routing strategies.

**63.** (B) (I), (III), and (IV)
ISDN Bearer (B) channels carry voice or data at 64 kbps and can be aggregated for higher bandwidth. The Delta (D) channel, operating at 16 or 64 kbps, is primarily used for signaling between switching equipment to manage calls. The claim that B-channels cannot be aggregated is incorrect, as this is a key feature used for applications needing more speed.

**64.** (C) Space out access points and limit to 20 users per point.
To prevent signal degradation and maintain performance in a large office, it is best to deploy multiple wireless access points that are appropriately spaced out. Limiting each access point to about twenty users helps ensure that the available bandwidth is not overextended. This distributed approach provides better coverage and a more reliable connection for all users than relying on a single point.

**65.** (C) Sub-oceanic transponder relays
Modern satellite communication leverages high throughput satellites and various orbital configurations, including medium-earth and low-earth orbits, to enhance network capabilities. Non-geostationary satellites also play a significant role. Sub-oceanic transponder relays, however, refer to undersea cable technology rather than satellite systems. Therefore, they are not an emerging satellite technology used by VSAT players for wide-area aerial communication.

**66.** (A) Provides wide-area wireless data communication to multiple points.
WiMAX is a wireless technology designed to provide high-speed data communication over large geographic areas, acting as a wireless alternative to cable and DSL. It can connect multiple points over several miles, making it suitable for metropolitan area networks. Unlike Wi-Fi, which is intended for local, short-range use, WiMAX provides a broader reach and can service hundreds of users simultaneously.

**67.** (C) Both (I) and (II)
When a dial-up remote access server needs more than two modems, a multi-port serial adapter is used to expand its capacity. This adapter is typically a PCI or ISA card that adds a large number of serial ports, allowing multiple modems to be pooled together. This setup enables the server to handle many simultaneous incoming calls from remote users efficiently.

**68.** (B) MPLS cloud technology
Many Indian banks have transitioned to Multiprotocol Label Switching (MPLS) cloud technology for their domestic and international connectivity. MPLS provides greater resiliency and better traffic management than traditional point-to-point leased lines. Although it can be more expensive, its ability to prioritize data and ensure reliable communication across a complex network of branches makes it a preferred choice for financial institutions.

**69.** (A) Virtual LAN (VLAN)
A Virtual LAN (VLAN) allows a network administrator to logically group devices together regardless of their physical location. This architecture decreases latency and enhances security by controlling traffic patterns through software configuration. However, since devices are logically on the same network, a virus can still spread through the entire VLAN if one system becomes infected, representing a significant security consideration.

**70.** (C) Amplify and retransmit the signal at a different frequency.
A satellite's transponder receives a weak signal from an earth station, amplifies it to increase its strength, and then retransmits it back to earth. To prevent the powerful outgoing transmission from interfering with the weak incoming signals, the transponder shifts the frequency of the signal. This frequency conversion is essential for maintaining clear and reliable two-way communication in satellite networks.

**71.** (B) (I), (II), (III), and (V)
Wi-Fi operates in various gigahertz bands and is intended for local area use. WiMAX is designed for much longer ranges, potentially up to forty miles, and can support hundreds of users. It often provides the backhaul internet connection for local Wi-Fi hotspots. The claim that Wi-Fi provides 70 Mbps over forty miles is incorrect, as Wi-Fi is a short-range technology.

Click Here to Buy book on Amazon

**72.** (D) Assertion (A) is false, but Reason (R) is true.
Frame relay is primarily based on Permanent Virtual Circuits (PVCs), which are "nailed" or fixed connections, although it can support Switched Virtual Circuits. Conversely, ISDN is a circuit-switched technology where connections are established on demand, much like a standard phone call. Therefore, the assertion about frame relay and the comparison to ISDN's connectivity requirements are both fundamentally misstated.

**73.** (D) P-4, Q-2, R-3, S-1
MPLS is often called "Layer 2.5" because it sits between the data link and network layers. Traditional router-centric strategies direct traffic using IP and access control lists. SD-WAN enables intelligent, application-aware routing through software. VLANs allow multiple networks to operate virtually as one, which helps in reducing latency. Matching these ensures a correct understanding of modern network architectures.

**74.** (C) P-4, Q-1, R-2, S-3
MPLS integrates Layer 2 and Layer 3 information to speed up traffic. SD-WAN is a virtual architecture that intelligently directs traffic to cloud services. VLANs let multiple networks work as a single LAN to reduce latency. Traffic engineering is the practice of setting the specific path that data will take. These features define how modern networks manage and optimize data flow.

**75.** (D) P-2, Q-1, R-4, S-3
Radio frequency covers electromagnetic radiation from 3 Hz to 300 GHz. WiMAX has a broad range of up to forty miles, whereas Wi-Fi is for shorter-range LAN applications with specific channel sizes. GSM technology is the basis for 3G and 4G connectivity used in network designs. Matching these attributes highlights the technical specifications and use cases for various wireless technologies.

**76.** (D) An ISDN device can communicate directly with non-ISDN devices.
Integrated Services Digital Network (ISDN) is a digital technology used for transmitting voice, video, and data over standard phone lines. Connections are made similarly to phone calls and billed by time and distance. However, an ISDN device cannot communicate directly with a non-ISDN device without some form of translation or gateway, as the underlying signaling and data formats differ significantly.

**77.** (B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
Wireless networks can reduce costs by eliminating the need for extensive physical cabling. It is also true that wireless signals weaken over distance and are affected by obstacles like metal or floors. While both statements are factually correct, the signal degradation mentioned in the reason does not explain why wireless networks are cheaper to operate than wired ones; that is due to installation.

**78.** (C) 22,300 miles
For a communications satellite to remain in a geosynchronous orbit, it must be positioned at a specific altitude where its orbital period matches the earth's rotation. This distance is approximately 22,300 miles above the equator. At this height, the satellite appears to stay in a fixed position in the sky, which is essential for consistent communication with fixed earth stations.

**79.** (B) Allows centralized configuration for separate geographical sites.
One major benefit of Virtual LANs (VLANs) is the ability to manage and configure network settings centrally for devices that may be in different physical locations. This logical grouping simplifies administration and allows for flexible network design without the need to physically rewire workstations. It does not eliminate viruses or use an immutable bus topology, but rather improves organizational agility.

**80.** (D) They prohibit the two-way transmission of data and voice.
VSAT networks provide numerous benefits for financial institutions, including online connectivity for remote branches and ATMs, and support for distance learning. A key feature of VSAT technology is its ability to support two-way transmission of both data and voice. Therefore, stating that VSAT prohibits two-way communication is incorrect, as that capability is fundamental to its role in banking operations.

Downloaded from www.pdf.tube

**81.** (C) Implementing a Token Ring directional token protocol.
Protecting a wireless network involves standard practices such as data encryption, multi-factor authentication, and systems to secure mobile devices. Token Ring is an older, wired network protocol that uses a specific token-passing mechanism to manage data transmission. It is not a security method designed for or recommended for protecting modern wireless networks from unauthorized access or data breaches.

**82.** (A) Combines channels into one faster connection as needed.
The ISDN Basic Rate Interface (BRI) consists of two Bearer (B) channels and one Delta (D) channel. A key capability of BRI is the ability to aggregate or combine the two 64 kbps B-channels to create a single, faster 128 kbps connection when higher bandwidth is required. This flexibility allows for better handling of data-intensive applications over digital lines.

**83.** (D) They prohibit the two-way transmission of data and voice.
VSAT technology is highly beneficial for banks because it enables reliable two-way communication for data and voice across geographically dispersed locations. It allows for the easy expansion of networks to include remote ATMs and facilitates staff training through interactive learning. The claim that it prohibits two-way transmission is false, as this functionality is a core requirement for modern banking infrastructure.

**84.** (C) Requires patch cords to be unplugged when a workstation moves.
VLANs are designed to provide flexibility by allowing network changes through software configuration rather than physical adjustments. One of their main advantages is that a workstation can be moved to a different physical port without needing to unplug or rearrange patch cords to stay on the same logical network. Therefore, the statement that moves require physical rewiring is incorrect for VLANs.

**85.** (D) 1997
Multiprotocol Label Switching (MPLS) is a technology that was developed to improve the efficiency of network routing by integrating Layer 2 link information with Layer 3 network information. The Internet Engineering Task Force (IETF) recognized the importance of this approach and formed a dedicated working group to standardize the technology in 1997, marking a significant milestone in network evolution.

**86.** (B) P-2, Q-3, R-4, S-1
In ISDN, the B-channel provides 64 kbps for data or voice, while the D-channel in a BRI setup handles signaling at 16 kbps. The Basic Rate Interface (BRI) provides two B-channels and one D-channel over a standard line. The Primary Rate Interface (PRI) offers much higher capacity with twenty-three B-channels and one D-channel over a high-speed link.

NODIA

**87.** (B) 8 to 12 users
For a wireless network to support Voice over IP (VoIP) or unified communications effectively, voice quality must be prioritized. Because voice traffic is sensitive to delays and jitter, it is recommended to limit the number of users to between eight and twelve per access point. This ensures sufficient bandwidth and low latency, preventing the degradation of audio during conversations.

**88.** (D) (I), (II), and (III)
Satellite communications utilize various frequency bands to transmit data. The C band typically operates at 6/4 GHz, the Ku band at 14/11 GHz, and the Ka band at 30/20 GHz. Each band has different characteristics regarding bandwidth and susceptibility to atmospheric interference like rain. All three listed bands and their corresponding frequencies are standard in the field of satellite network technology.

**89.** (B) (I), (III), and (IV)
SD-WAN securely connects users to applications by utilizing various transport services like MPLS and broadband. It intelligently directs traffic to cloud providers and helps lower IT expenses while increasing productivity. Unlike older models that rely on rigid access control lists, SD-WAN uses software to provide a more flexible and application-aware approach to managing wide-area network traffic and security.

**90.** (D) Assertion (A) is false, but Reason (R) is true.
Multiprotocol Label Switching (MPLS) does not direct data based on long IP addresses; instead, it uses short path labels to forward packets. This label-based switching is efficient because it avoids the need for complex, time-consuming lookups in a traditional routing table at every hop. Therefore, while the reason accurately describes the benefit of labels, the assertion about IP-based routing is incorrect.

**91.** (B) Star Topology
In a star topology, all nodes are individually connected to a central hub or switch. This design is cable-efficient since each node only needs one link to the center. However, the central hub represents a single point of failure; if it malfunctions, all attached nodes lose their ability to communicate, effectively disabling the entire local network segment.

**92.** (C) Logical AND
To determine the network address from an IP address, a bitwise logical AND operation is performed with the subnet mask. This process masks the host portion of the address, leaving only the bits that represent the network. The result allows routers to identify which subnetwork a packet belongs to, facilitating the correct delivery of data across a complex internetwork.

**93.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
The OSI model is defined by seven distinct layers, whereas the TCP/IP model is often viewed as having four. This difference arises because the TCP/IP model combines several OSI layers. Specifically, the physical and data link layers of OSI are often clubbed together as a single network interface layer in the TCP/IP model, leading to the four-layer representation.

**94.** (C) IPv4 header is 20 bytes (13 fields); IPv6 is 40 bytes (8 fields).
The IPv4 header is typically twenty bytes long and contains thirteen different fields. In contrast, the IPv6 header has been redesigned to be more efficient, consisting of forty bytes but only eight fields. This streamlined structure in IPv6 helps routers process packets more quickly, even though the total header size is larger due to the much longer 128-bit addresses.

**95.** (B) Packets skip computers, making it faster than Star topology.
In a ring topology, each packet must pass through every computer between the source and the destination, which actually makes it slower than a star topology where data goes through a central hub. Advantages include better performance under heavy loads compared to bus topologies and the lack of a need for a central server to manage the connections between nodes.

**96.** (C) 200.133.175.31
In a subnet starting at 200.133.175.16 with a 4-bit subnet mask, there are sixteen possible addresses (2 raised to the power of 4). The range for this subnet is from .16 to .31. The first address (.16) is the network address, and the last address (.31) is the broadcast address, which cannot be assigned to an individual host node.

**97.** (D) Includes Session and Presentation within the Application layer.
The TCP/IP reference model differs from the seven-layer OSI model by having a broader Application layer. This single layer in the TCP/IP stack encompasses the functions that the OSI model separates into the Application, Presentation, and Session layers. By merging these three, the TCP/IP model simplifies the process for developers who are creating network-aware software and communication protocols.

**98.** (B) Classful IPv4 → Classless Inter-Domain Routing (CIDR) → IPv6
The evolution of internet addressing began with the rigid classful IPv4 system (Classes A, B, and C). As IP addresses became scarce, Classless Inter-Domain Routing (CIDR) was introduced in the 1990s to allow for more flexible and efficient allocation. Finally, IPv6 was developed and deployed to provide a much larger address space for the long-term growth of the internet.

**99.** (C) Enforces rigid Class A, B, and C boundaries for IPv4.
Classless Inter-Domain Routing (CIDR) was specifically introduced to replace the old, inefficient classful addressing system. Instead of being restricted by rigid Class A, B, or C

Click Here to Buy book on Amazon

boundaries, CIDR uses variable-length subnet masking. This allows for the allocation of IP address blocks based on prefixes of arbitrary length, which greatly improves the scalability and efficiency of routing on the internet.

**100.** (C) Tree Topology
A tree topology is a hierarchical network structure where multiple star networks are connected to a central main bus cable. This design combines the characteristics of both bus and star topologies. It allows for easy expansion of the network by adding more star segments, making it suitable for larger organizations that need a structured and scalable cabling system for communications.

**101.** (A) It allows more efficient aggregation of subnetwork prefixes.
IPv6 was designed with a hierarchical addressing structure that enables more efficient aggregation of subnetwork prefixes by Internet Service Providers. By grouping multiple small networks under a single larger prefix in routing tables, the total number of entries that routers must store is reduced. This approach helps manage the growth of global routing tables as the number of connected devices increases.

**102.** (A) There is a central computer or server to which all the workstations are directly connected to control connectivity.
A ring topology is defined by workstations connected in a closed loop where data travels from one node to the next. It does not utilize a central computer or server to control connectivity for all workstations; that is the characteristic of a star topology. In a ring, each node acts as a repeater, passing the signal along until it reaches its destination.

**103.** (B) P-2, Q-1, R-4, S-3
In classful addressing, Class A uses the default subnet mask 255.0.0.0, Class B uses 255.255.0.0, and Class C uses 255.255.255.0. Class D is reserved for multicasting and does not use a traditional subnet mask for host identification. Correctly matching these classes to their masks is fundamental to understanding how IPv4 networks were originally structured and divided into network and host portions.

**104.** (D) P-3, Q-4, R-1, S-2
IPv4 addresses are divided into classes based on their first octet. Class A ranges from 1 to 126, Class B from 128 to 191, Class C from 192 to 223, and Class D, used for multicasting, from 224 to 239. Address 127 is reserved for loopback testing. Matching these ranges is essential for identifying the default network type and size of a given IP.

**105.** (C) P-3, Q-2, R-1, S-4
IPv4 is divided into classes A through E, and its header consists of thirteen fields over twenty bytes. IPv6 uses 128-bit addresses and replaces subnet masks with a prefix and identifier system. The IPv6 address itself is four times larger than an IPv4 address. These characteristics highlight the architectural differences between the two main versions of the Internet Protocol used today.

**106.** (B) User Datagram Protocol (UDP)
The User Datagram Protocol (UDP) is a member of the TCP/IP suite that provides a simple, connectionless delivery service. Unlike TCP, which ensures reliable data arrival, UDP sends packets without establishing a session or guaranteeing delivery. This makes it suitable for applications like messaging or streaming where speed is prioritized over the perfect reconstruction of the data stream at the destination.

**107.** (A) Increases address size to 128 bits, providing $3.4 \times 10^{38}$ IPs.
IPv6 significantly expands the available address space by increasing the address size from 32 bits to 128 bits. This change provides approximately $3.4 \times 10^{38}$ unique IP addresses, which is an astronomical number compared to the 4.3 billion offered by IPv4. This vast pool of addresses is intended to accommodate the explosive growth of internet-connected devices for the foreseeable future.

**108.** (B) (I), (III), and (IV)
In a full mesh topology, every workstation is directly connected to every other node, allowing it to handle high traffic and provide redundancy. If one node fails, the rest of the network remains functional. However, the complexity and the number of connections required make it very expensive to implement. The claim that one broken node brings the entire network down is incorrect.

NODIA

**109.** (D) Node addresses consisting of all "0"s are reserved for specifying the local network address. In any IP subnet, certain addresses are reserved for specific functions. A node address where all the host bits are "0" is used to identify the local network itself rather than a specific device. Similarly, a node address with all "1"s is used for broadcasting to every device on that subnet. These restrictions ensure that network communications can be routed correctly.

**110.** (C) It is a Class B address; Network part is `140.179.x.x`, Node part is `x.x.220.200`.
The IP address 140.179.220.200 falls within the Class B range (128 to 191). By default, a Class B address uses the first two octets for the network portion and the last two octets for the node portion. Therefore, for this specific address, the network part is 140.179.x.x and the node or host part is x.x.220.200, according to classful addressing rules.

**111.** (B) (I), (II), (III), and (IV)
Subnetting is used to organize different physical media, preserve limited address space, and implement security measures within a network. It also helps minimize network traffic by confining local data packets to their specific segment. However, subnetting is a process within a specific protocol version like IPv4; it is not a method for dynamically converting 32-bit IPv4 addresses into 128-bit IPv6 addresses.

**112.** (B) Application → lower layer adding header/footer → physical layer → transmitted through cable
When an application sends a request, the data moves down the layers of the communication model. Each lower layer adds its own header or footer containing control information, a process known as encapsulation. Finally, the data reaches the physical layer, where it is converted into signals for transmission through a cable to the destination host, which then reverses the entire process.

**113.** (C) Assertion (A) is true, but Reason (R) is false.
It is true that star topologies make it easy to detect faults and add or remove devices without disrupting the rest of the network. However, the reason provided is incorrect; the feature of every workstation being connected to every other one in a closed loop describes a mesh or ring topology, not a star topology, which uses a central hub.

**114.** (C) 4 bits
To create fourteen subnets, you need to determine the number of bits required using the formula ($2^n$ – 2). With 4 bits, you get ($2^4$ – 2), which equals fourteen available subnets. This mask extension allows an organization to divide its Class C network into the required number of smaller segments, each capable of supporting its own set of host nodes.

**115.** (D) 172.16.0.0/12
Private IP address ranges are reserved for use within internal networks and are not forwarded by public internet routers. One such valid block is 172.16.0.0 through 172.31.255.255, which is represented by the 172.16.0.0/12 prefix. Other standard private blocks include 10.0.0.0/8 and 192.168.0.0/16. Using these addresses behind a NAT gateway allows multiple local devices to share a single public IP.

**116.** (C) Both (I) and (II)
Physical topology refers to the actual, visible arrangement of cables and workstations in a network. Logical topology, or signal topology, describes the conceptual path that signals take as they travel from one node to another. A network can have a physical star layout while operating with a logical ring signal path, making it important to distinguish between these two concepts.

**117.** (B) 6 subnets
Using a 3-bit subnet mask extension, the number of available subnets is calculated with the formula ($2^n$ – 2). Since 2 raised to the power of 3 is 8, subtracting 2 results in 6 usable subnets. The two subnets are subtracted because, in legacy network environments, the subnets consisting of all "0"s and all "1"s were often reserved and not used.

**118.** (D) A Linear Bus topology requires terminators at both ends of the backbone cable.
In a linear bus topology, all devices are connected to a single backbone cable. To prevent signals from reflecting back and causing interference, terminators must be installed at both ends of this cable. Star topologies generally require more

Downloaded from www.pdf.tube

cable than bus layouts. A tree topology connects multiple star networks to a bus, and only full mesh networks connect every node directly.

**119.** (A) A 3-bit subnet mask provides exactly 8 available subnets for use in legacy environments. The formula for calculating available subnets is $(2^n - 2)$, which accounts for the reserved network and broadcast addresses. Therefore, a 3-bit mask provides 6 available subnets, not 8. Subnetting is used to manage traffic by controlling collisions and requires subtracting two from the total possible combinations to identify the usable range for host nodes and subnetwork identifiers in traditional IP networking.

**120.** (A) (I) and (II) only
IPv4 addresses are 32-bit numbers often shown as four decimal values, and the 127.x.x.x range is reserved for loopback testing. IPv6 addresses are 128 bits and are typically represented as eight groups of hexadecimal digits, not decimal values. Therefore, the first two statements correctly describe IPv4 characteristics, while the third statement misidentifies the standard representation format for IPv6.

**121.** (C) Classful network design → Classless Inter-Domain Routing (CIDR) → IPv6 deployment
The Internet's addressing system began with a rigid classful design that quickly proved inefficient as the network grew. To manage the depletion of available IP addresses, Classless Inter-Domain Routing (CIDR) was introduced to allow for more flexible allocations. Finally, IPv6 was developed as a long-term solution, offering a massive increase in address space to support the future of digital connectivity.

**122.** (C) IPv6 supports native encryption and authentication features.
One of the key improvements in IPv6 over IPv4 is the inclusion of mandatory support for IPsec, which provides native encryption and authentication for network traffic. While security can be added to IPv4, it was not part of the original protocol design and is not inherently enforced across all links. IPv6's built-in security features ensure a more secure foundation for global communication.

**123.** (C) The term subnet mask is used exclusively within IPv6 routing protocols.
A subnet mask is a fundamental concept in IPv4 networking used to distinguish between the network and host portions of an IP address. It uses "1"s for network bits and "0"s for host bits. While IPv6 uses a similar concept called a prefix length, the term "subnet mask" is not used exclusively within IPv6; it is primarily associated with IPv4.

**124.** (B) (I), (II), (III), and (IV)
The TCP/IP suite includes IP for routing, TCP for reliable transmission, and UDP for faster, unguaranteed delivery. The bottom layers are often combined into a single host-to-network layer. However, the TCP/IP model does not separate the session and presentation layers; instead, it incorporates their functions into the Application layer, making the fifth statement in the provided list incorrect.

**125.** (B) 224.0.0.0/4
Private IP addresses, such as the 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 blocks, are reserved for internal use within organizations. The 224.0.0.0/4 range is not a private address block; instead, it is designated as Class D for multicast traffic on the public internet. These multicast addresses are used for one-to-many communication rather than for identifying nodes on a private local area network.

NODIA

# CHAPTER 05
# Introduction to Information Systems

**May/June 2013**

**1.** Which of the following statements regarding the Design & Development stage of the SDLC is incorrect?
(A) System elements such as screens and reports are designed using methods like prototyping.
(B) Computer-Aided Software Engineering (CASE) tools are utilised during this stage.
(C) Development tools and the deployment environment are selected for the target platform.
(D) Costs are projected for the first time during testing rather than the design phase.

**Oct/Nov 2024**

**2.** Which of the following statements correctly distinguishes acquisition projects from development projects?
(A) Acquisition projects bypass the planning stage entirely and move directly to the implementation phase.
(B) Acquisition projects do not require management to define functional and security requirements for the system.
(C) Acquisition projects replace the SDLC design and development phases with a bid solicitation process.
(D) Acquisition projects utilize the waterfall model exclusively for vendor selection and contract finalization.

**May/June 2006**

**3.** When employees identify a gap between a current state of affairs and a desired state of affairs, the process they undertake to structure a series of decisions and choices is known as:
(A) System Analysis
(B) Procedural Formulation
(C) Problem Solving
(D) Data Integration

**Oct/Nov 2012**

**4.** Identify the correct pair representing a specific CASE tool type and its corresponding software example:
(A) Quality Assurance Tools - EPF Composer, Doxygen
(B) Web Development Tools - Accept 360, Accompa
(C) Configuration Management Tools - Fossil, Git, Accu REV
(D) Analysis Tools - SoapTest, JMeter

**May/June 2021**

**5.** Consider the following statements regarding network setups:
I. In a centralized network, dumb terminals perform necessary calculations and format the output before sending it to the mainframe.
II. In a distributed network, departmental mini-computers are used to run applications and may communicate periodically with a central mainframe.
Which of the above statement(s) is/are correct?
(A) Only I
(B) Only II
(C) Both I and II
(D) Neither I nor II

**Oct/Nov 2005**

**6.** In the following question, a statement of Assertion (A) is followed by a statement of Reason (R):
Assertion (A): Quality Assurance (QA) tools ensure conformance of quality as per organization standards during software development.
Reason (R): QA tools consist solely of automatic logging and root cause analysis mechanisms for post-delivery modifications.
Select the correct answer:
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).

Click Here to Buy book on Amazon

(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2017**

**7.** What is defined as the gobs of text and numbers that an organization gathers in the course of doing business, which does not do the firm any good until analyzed?
(A) Information
(B) Data
(C) System input
(D) Strategic intelligence

**Oct/Nov 2023**

**8.** In the following question, a statement of Assertion (A) is followed by a statement of Reason (R):
Assertion (A): There is a clear trend towards buying software packages rather than developing custom software.
Reason (R): Packages are less expensive, immediately available, and the MIS department does not have to provide all the support for the program.
Select the correct answer:
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2009**

**9.** What is the most appropriate primary benefit of utilizing CASE tools during the Software Development Life Cycle?
(A) To eliminate the need for end-user documentation and training manuals through automated help systems.
(B) To accelerate the development of the project and help uncover flaws before moving ahead with the next stage.
(C) To replace the human decision-making process during the design phase completely with AI modules.
(D) To restrict the development environment to only machine languages and low-level hardware instructions.

**Oct/Nov 2019**

**10.** Match the programming languages in List I with their respective characteristics or generations in List II:
List I: Programming Language
P. Assembly language
Q. FORTRAN
R. SQL
S. Oracle Forms
List II: Characteristic or Generation
1. 4GL/5GL used for database queries
2. Second generation language
3. 4GL used as a development tool
4. 3GL developed for science & engineering
(A) P-1, Q-3, R-4, S-2
(B) P-4, Q-1, R-2, S-3
(C) P-2, Q-4, R-1, S-3
(D) P-3, Q-2, R-1, S-4

**May/June 2015**

**11.** Which updating mode is applied to a master file as the transactions happen, ensuring the information is always up to date?
(A) Batch processing mode
(B) Sequential processing mode
(C) Periodic processing mode
(D) Interactive or real time mode

**Oct/Nov 2007**

**12.** Consider the following stages of the Systems Development Life Cycle (SDLC):
I. Operation & maintenance
II. Planning and analysis
III. Implementation
IV. Design & development
V. Testing & acceptance
Arrange the stages in the correct chronological order:
(A) II, IV, III, V, I
(B) II, III, IV, V, I
(C) II, IV, V, III, I
(D) II, V, IV, III, I

**May/June 2025**

**13.** Consider the following statements regarding deployment strategies:
I. In parallel deployment, the old system and new system run concurrently for some time.
II. In phased deployment, the new system is introduced in phases rather than the whole system at a time.

NODIA

III. In pilot deployment, the whole system is introduced to a subset of the organization to be tested over a period of time.
IV. In parallel deployment, the old system is immediately discontinued once the new system is installed.

Which of the above statement(s) is/are correct?
(A) I, II, and III
(B) II, III, and IV
(C) I, III, and IV
(D) I, II, and IV

**Oct/Nov 2014**

**14.** Consider the following statements regarding communication standards:
I. The underlying communication standard of the Internet is TCP/IP.
II. Proprietary standards are set by committees of people from multiple companies.
III. The standards used on the Internet are open standards.

Which of the above statement(s) is/are correct?
(A) I and II
(B) II and III
(C) I and III
(D) I, II, and III

**May/June 2011**

**15.** A software development team is providing an initial look and feel of a product to users to simulate hardware-independent user interfaces based on existing information. Which specific type of CASE tools are they utilizing?
(A) Configuration Management Tools
(B) Programming Tools
(C) Maintenance Tools
(D) Prototyping Tools

**Oct/Nov 2020**

**16.** Which of the following defines a system that takes inputs, completes its processing, and produces outputs?
(A) Information System
(B) Decision Support System
(C) Transaction Processing System
(D) Database Management System

**May/June 2008**

**17.** Consider the following statements about various CASE tools:
I. Diagram tools represent system components and data flow in a graphical form.
II. Process Modelling tools help managers choose or modify a software process model.
III. Project Management tools help in cost and effort estimation, and real-time project information sharing.
IV. Analysis tools automatically check for inconsistency, inaccuracies, and data redundancies.
V. Documentation tools generate documents solely for end-users, excluding in-house professionals.

Which of the above statement(s) is/are correct?
(A) I, II, III, and V
(B) I, II, III, and IV
(C) II, III, IV, and V
(D) I, III, IV, and V

NODIA

**Oct/Nov 2018**

**18.** Which of the following is not classified as a third-generation programming language (3GL)?
(A) Prolog
(B) Java
(C) Pascal
(D) Python

**May/June 2022**

**19.** Which of the following statements regarding acquisition tools is incorrect?
(A) Invitations-to-tender involve soliciting bids from vendors when acquiring hardware or integrated systems.
(B) Request-for-proposals involve soliciting bids when acquiring off-the-shelf or third-party developed software.
(C) Acquisition of off-the-shelf software requires less stringent evaluation procedures than acquiring software specifically designed for financial purposes.
(D) The risks associated with using general business purpose software are typically higher than those for financial applications.

**Oct/Nov 2010**

**20.** Match the models of software development in List I with their descriptions in List II:
List I: Model
P. Waterfall
Q. Spiral
R. Prototype
S. Packages
List II: Description
1. User specifies part of the system,

development team builds it, then user specifies another part.
2. Less expensive, immediately available, and supported by the corporation that sells them.
3. User specifies the entire system upfront, which is handed off to the development team.
4. Team makes a simple version, user reacts, and the team modifies it repeatedly.

(A) P-3, Q-1, R-4, S-2
(B) P-1, Q-2, R-3, S-4
(C) P-4, Q-3, R-2, S-1
(D) P-2, Q-4, R-1, S-3

**May/June 2014**

**21.** Identify the incorrect pair matching the type of CASE tool with its practical application:
(A) Maintenance Tools - Automatic error ticket generation
(B) Programming Tools - IDE and simulation features
(C) Design Tools - Checking for data redundancies and erroneous omissions
(D) Documentation Tools - Creating system and training manuals

**Oct/Nov 2025**

**22.** Which of the following correctly identifies activities involved in the Planning and Analysis stage of the SDLC?
(A) Defining the problem, conducting a feasibility study, and selecting the initial deployment environment
(B) Organizing the project team, gathering business requirements, and defining system performance criteria
(C) Selecting programming languages, creating a high-level project plan, and developing prototype screens
(D) Defining the problem, conducting unit testing, and creating detailed process flow diagrams

**May/June 2005**

**23.** Identify the correct pair regarding operating systems and their primary support characteristics:
(A) UNIX/LINUX - Provides robust support for graphics processing and advanced multimedia applications
(B) Macintosh - Provides robust support for distributed computing and enterprise network management
(C) Macintosh - Handles centralized keystrokes for mainframe processing and legacy terminal emulation
(D) UNIX/LINUX - Provides robust support for communication tasks and distributed computing

**Oct/Nov 2016**

**24.** Match the categories of CASE tools in List I with their corresponding SDLC stages in List II:
List I: CASE Tool Category
P. Upper Case Tools
Q. Lower Case Tools
R. Integrated Case Tools
S. Central Repository
List II: SDLC Stage
1. Helpful in all stages from requirement gathering to testing and documentation.
2. Serves as a data dictionary and stores requirement documents.
3. Used in implementation, testing, and maintenance.
4. Used in planning, analysis, and design stages.

(A) P-3, Q-4, R-2, S-1
(B) P-1, Q-2, R-3, S-4
(C) P-2, Q-1, R-4, S-3
(D) P-4, Q-3, R-1, S-2

**May/June 2019**

**25.** A software development team is fixing product defects and retesting the software until it reaches the quality standards defined in the Software Requirement Specification. Which SDLC stage is primarily being executed?
(A) Design & Development
(B) Testing & Acceptance
(C) Planning and Analysis
(D) Operation & Maintenance

**Oct/Nov 2011**

**26.** Which of the following comprises all five parts of an information system?
(A) Hardware, Software, Network, Database, and Personnel
(B) Inputs, Processing, Outputs, Storage, and Control
(C) Planning, Analysis, Design, Implementation, and Maintenance
(D) Hardware, Software, Data, People, and

Downloaded from www.pdf.tube

Procedures

May/June 2007

**27.** Which of the following is not a function typically performed by Change Control Tools?
(A) Providing live previews of web pages
(B) Automating file management
(C) Automating code management
(D) Enforcing the change policy of the organization

Oct/Nov 2022

**28.** What is the most appropriate reason for utilising a development environment that includes CASE tools?
(A) To coordinate group programmers, manage large projects, and analyze programs.
(B) To bypass the requirement for a compiler or interpreter entirely during code development.
(C) To convert fourth-generation languages directly into low-level machine language code.
(D) To distribute the processing load between the central mainframe and user terminals efficiently.

May/June 2018

**29.** A bank's software project managers and analysts use a tool that requires a central place of storage where product specifications, requirement documents, and a data dictionary are kept to ensure consistent information. What is this component called?
(A) Upper CASE
(B) Integrated Database
(C) Central Repository
(D) Enterprise Information System

Oct/Nov 2015

**30.** A financial institution is acquiring new software for its branch operations. The management evaluates compatibility with existing hardware, speed, error handling, ease of use, and annual maintenance price. Which stage of the SDLC is the institution currently executing?
(A) Planning and Analysis
(B) Design & Development
(C) Testing & Acceptance
(D) Implementation

May/June 2024

**31.** In the following question, a statement of Assertion (A) is followed by a statement of Reason (R):
Assertion (A): Top management should be most fully supplied with information concerning the external environment of the bank.
Reason (R): Top management requires detailed operational data about internal procedures to monitor daily branch activities.
Select the correct answer:
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Oct/Nov 2017

**32.** Which of the following is not an essential characteristic of a Decision Support System (DSS)?
(A) Support decision making for solving structured, semi-structured, and unstructured problems.
(B) A rigid system structure that prevents adaptation to changing conditions over time.
(C) Integrated subsystems allowing managers to retrieve information along broader, functional lines.
(D) Output directed to organization personnel at all levels, including lower management.

NODIA

May/June 2012

**33.** An airline reservation system updates seat availability the moment a booking is confirmed. Which type of system and updating mode is being utilized?
(A) MIS with batch updating
(B) TPS with interactive updating
(C) TPS with batch updating
(D) DSS with real time updating

Oct/Nov 2008

**34.** What is the definition of Groupware?
(A) Software that automates the SDLC testing and acceptance phase through automated scripts and tools.
(B) Hardware that processes large volumes of

numerical data sequentially in a centralized server room.
(C) An operating system service that manages computer hardware resources exclusively for single-user tasks.
(D) Software that helps groups of people work together more efficiently and effectively by enabling collaborative computing.

**May/June 2023**

**35.** Consider the following characteristics of information:
I. Simulated 'what if' information of a long-term nature.
II. Descriptive-historical information.
III. Competitive actions and availability of resources.
IV. Accent on exception reporting.
Which of the above statements correctly describe the essential characteristics of Strategic Information?
(A) I and II
(B) I and III
(C) II and IV
(D) III and IV

**Oct/Nov 2006**

**36.** In the following question, a statement of Assertion (A) is followed by a statement of Reason (R):
Assertion (A): GDSS provides automated means to enter, record, and build on team members' ideas.
Reason (R): GDSS capabilities include alternative generation, issue interpretation, and anonymous electronic recording.
Select the correct answer:
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2020**

**37.** Which of the following represent the three major types of information systems?
(A) TPS, MIS, and DSS
(B) TPS, MIS, and GDSS
(C) MIS, DSS, and EIS
(D) TPS, DSS, and EIS

**Oct/Nov 2013**

**38.** Consider the following statements regarding the characteristics of a DSS:
I. Broad-based approach to supporting decision making (management by perception).
II. Human/machine interface where human retains control.
III. Support for solving only highly structured problems.
IV. Utilization of appropriate mathematical and statistical models.
V. Query capabilities to obtain information by request-interactive mode.
Which of the above statement(s) is/are correct?
(A) I, II, III, and IV
(B) I, II, IV, and V
(C) II, III, IV, and V
(D) I, III, IV, and V

**May/June 2010**

**39.** A senior manager at a bank requires immediate access to information concerning factors critical to accomplishing the organization's strategic objectives. Which system is specifically tailored to present this multidimensional information according to the executive's preferences?
(A) TPS
(B) MIS
(C) GDSS
(D) EIS

**Oct/Nov 2009**

**40.** Which of the following statements regarding Operational Information is incorrect?
(A) It is needed at the lowest level of decision making.
(B) It allows line managers to measure performance against predetermined objectives.
(C) It provides feedback that keeps higher levels of management aware of favourable and unfavourable results.
(D) It assists top management in strategic decisions characterized by a great deal of uncertainty.

Click Here to Buy book on Amazon

May/June 2016

**41.** In which of the following business applications is a Group Decision Support System (GDSS) typically found?
(A) Processing payroll in batch mode.
(B) Training decision makers to deal with disaster situations or high-risk situations.
(C) Managing individual executive calendars.
(D) Tracking individual bugs during the maintenance phase of SDLC.

Oct/Nov 2021

**42.** How does a Decision Support System (DSS) fundamentally differ from a traditional Management Information System (MIS)?
(A) A DSS handles routine master file updates, whereas an MIS provides interactive query tools for users.
(B) A DSS is strictly used for batch processing operations, whereas an MIS operates in a real time mode.
(C) A DSS provides support for semi-structured decisions using highly interactive analytical models, whereas an MIS helps users identify problems.
(D) A DSS replaces the human decision-maker entirely, whereas an MIS only summarizes simple data sets.

May/June 2013

**43.** In the following question, a statement of Assertion (A) is followed by a statement of Reason (R):
Assertion (A): In a Decision Support System, the utilization of CRT terminals provides the decision maker the capability to manipulate and present data in a human/machine dialogue.
Reason (R): Throughout the interface, the decision maker surrenders control over the decision-making process to the machine.
Select the correct answer:
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

NODIA

Oct/Nov 2024

**44.** In a Decision Support System (DSS), why is the system designed to support an executive's skills rather than make the decision independently?
(A) Because DSS lacks the capability to store on-line information for extended periods within the database.
(B) Because DSS models can only handle highly structured decisions that do not require human intervention.
(C) Because human/machine interfaces cannot process mathematical models without external software support.
(D) Because professional judgment and insight are critical in decision making.

May/June 2006

**45.** A committee uses a system equipped with advanced presentation devices and software that calculates weights of decision alternatives and anonymously records ideas to solve organizational problems. What technology is primarily being utilized?
(A) Expert System (ES)
(B) Transaction Processing System (TPS)
(C) Group Decision Support System (GDSS)
(D) Executive Information System (EIS)

Oct/Nov 2012

**46.** Consider the following statements regarding the Transaction Processing System (TPS):
I. Payroll is an example of transactions that are generally handled in real time mode.
II. With batch updates, the computer and network are used more efficiently.
Which of the above statement(s) is/are correct?
(A) Only I
(B) Only II
(C) Both I and II
(D) Neither I nor II

May/June 2021

**47.** Which of the following terms are also used to refer to Executive Information Systems (EIS) as they gradually become widely used by managers, analysts, and other knowledge workers?
(A) Transaction Processing Systems and Enterprise Routing Systems
(B) Everyone's Information Systems and Enterprise Information Systems
(C) Global Decision Systems and Tactical Management Systems

(D) Broad-based Systems and Unified Management Systems

Oct/Nov 2005

**48.** Which of the following correctly describes Tactical Information?
(A) It is used to cover a long time span, generally one to five years, for senior management planning.
(B) It covers relatively short periods, not greater than 12 months, and is used to implement strategic plans at the functional levels.
(C) It involves structured and repetitive activities measurable in terms of specific results at the lowest level.
(D) It is characterized by predictive information concerning long-term trends and external market factors.

May/June 2017

**49.** Which of the following statements regarding DSS Integrated Subsystems is incorrect?
(A) Integrated subsystems process data for use along traditional, narrow departmental lines.
(B) Integrated subsystems process data for use along broader, functional lines.
(C) They allow managers to retrieve and manipulate information of concern to them.
(D) They support decisions by transcending isolated departmental data.

Oct/Nov 2023

**50.** Consider the following statements regarding the components of a DSS:
I. The Database Management System (DBMS) may contain both internal data generated by TPS/MIS and external data.
II. The Model Management System stores models used for analyzing financial health or forecasting demand.
III. Support Tools are designed specifically to restrict user interaction to batch processing.
Which of the above statement(s) is/are correct?
(A) I and II
(B) II and III
(C) I and III
(D) I, II, and III

May/June 2009

**51.** Which of the following best describes the specific support GDSS software provides to the group, in addition to individual workstation facilities?
(A) It restricts access to internal databases to prevent data redundancy and ensure strict security protocols.
(B) It automatically finalizes strategic decisions without human intervention to speed up the management process.
(C) It limits parallel communication to ensure strict sequential decision making across all functional departments.
(D) It provides capabilities for summarizing, aggregating and collecting results, ranking opinions, and prioritizing tasks.

Oct/Nov 2019

**52.** Match the levels of management in List I with their corresponding informational needs in List II:
List I: Management Level
P. Top Management
Q. Middle Management
R. Lower Management
List II: Informational Needs
1. Comprehensive reports, basically planning/control oriented.
2. Detailed reports, generally control oriented.
3. Overall reports, fundamentally planning oriented.
(A) P-1, Q-2, R-3
(B) P-2, Q-3, R-1
(C) P-3, Q-2, R-1
(D) P-3, Q-1, R-2

May/June 2015

**53.** What is the most appropriate explanation for why lines between categories of managerial decision making are blurred in practical situations?
(A) Strategic information is identical to operational information in modern, high-tech digital banking environments.
(B) Systems analysts cannot design information systems to separate any individual data points within the network.
(C) Different kinds of decision making require differing but overlapping informational requirements based on the level of the decision maker.
(D) Lower management is solely responsible for determining long-range policies and organizational goals in firms.

Downloaded from www.pdf.tube

# STUDYING FROM PDFs?

# THINK AGAIN.

If you are studying only from PDFs,
you are wasting valuable time.

Research shows that learning from

**PRINTED BOOKS** has up to

**4× HIGHER RETENTION**

than studying from screens.

**PRINT BOOK = BETTER MEMORY**

**PDF = LOWER RETENTION**

Those who study from **PRINTED BOOKS**
move **AHEAD.**

Others are left **BEHIND**
in competition.

In competitive exams,
being average is not enough.

## STAY ONE STEP AHEAD.

Oct/Nov 2007

**54.** What is the most appropriate reason why providing user-specific presentation capabilities in a conventional MIS is considered very expensive to implement compared to an EIS?
(A) MIS rely entirely on external data sources for providing decision support to senior executives.
(B) MIS do not utilize computer storage and require manual data entry for all reporting functions.
(C) MIS cater to a much larger user group dealing with structured and simpler problems.
(D) MIS are exclusively used for batch mode transaction updates for routine administrative processes.

May/June 2025

**55.** Consider the following characteristics of a DSS:
I. Output directed to organization personnel at all levels.
II. Integrated subsystems capable of processing data along broader functional lines.
III. Comprehensive data base utilizing a DBMS.
IV. Easy-to-use approach requiring extensive programming knowledge by the user.
V. Adaptive system over time, taking a few weeks to several months to effect system changes.
Which of the above statement(s) is/are correct?
(A) I, II, III, and V
(B) I, II, IV, and V
(C) II, III, IV, and V
(D) I, III, IV, and V

Oct/Nov 2014

**56.** What is defined as an information system used for decision-making and visualization of information that helps users identify problems without necessarily providing problem-solving facilities?
(A) Management Information System (MIS)
(B) Decision Support System (DSS)
(C) Executive Information System (EIS)
(D) Transaction Processing System (TPS)

May/June 2011

**57.** Match the collaborative computing software in List I with its primary category or examples in List II:
List I: Collaborative Software
P. E-mail and calendar programs
Q. Lotus Notes and Novell Groupwise
R. Brainstorming tools
S. Video conferencing
List II: Category or Example
1. Examples of groupware applications
2. Synchronous groupware components
3. GDSS alternative generation capabilities
4. Software associated with collaborative computing
(A) P-4, Q-1, R-3, S-2
(B) P-1, Q-2, R-4, S-3
(C) P-3, Q-4, R-1, S-2
(D) P-2, Q-3, R-1, S-4

NODIA

Oct/Nov 2020

**58.** A branch manager compares the daily transaction counts and deposit volumes against the budgeted figures to control operations. What type of information is primarily being utilized?
(A) Operational Information
(B) Strategic Information
(C) External Information
(D) Tactical Information

May/June 2008

**59.** Which of the following accurately describes the primary purpose of an Executive Information System (EIS)?
(A) To handle routine daily transactions such as paying bills and receiving goods from various suppliers.
(B) To measure performance against predetermined objectives for lower-level branch managers and staff.
(C) To serve the information needs of managers at the highest organizational levels by combining internal and external data.
(D) To develop process models and generate programming code automatically for the software engineers.

Oct/Nov 2018

**60.** A bank management implements a DSS across multiple branches to solve myriad problems. What economic factor most appropriately justifies the adoption of distributed decision support systems?
(A) The increasing cost of centralized mainframes and high-end server maintenance in the financial sector.
(B) The rapidly decreasing costs of computer storage and improvements in DBMS.

(C) The rising expense of hiring data entry personnel and administrative staff for large-scale operations.
(D) The elimination of the need for personnel in the data processing budget for all departmental functions.

**May/June 2022**

**61.** Once a PERT network is finished, what is the significance of the critical path?
(A) It is the shortest path through the network where tasks can be delayed without affecting the end date.
(B) It is the path that requires the least amount of resources and capital to complete the project.
(C) It is the longest path through the network where no task can be held up without delaying the completion of the project.
(D) It is a sequence of tasks that operate independently of any precedence relationship or dependencies.

**Oct/Nov 2010**

**62.** Which of the following is a correct statement regarding the Repeatable Level (Level 2) of CMM?
(A) The organization must put into place basic project management practices such as estimating software size and resources.
(B) The organization is no longer highly dependent on individuals for the success of a complex software project.
(C) The process belongs exclusively to the organization, not to individuals working within specific teams.
(D) The primary focus shifts entirely from product quality to process quality for continuous improvement cycles.

**May/June 2014**

**63.** A project manager is plotting project activities against a time frame using horizontal bars to show the duration of tasks. The left end of the bar shows the beginning of the task and the right end shows its finish. Which tool is being used?
(A) Gantt Chart
(B) PERT Chart
(C) Flow Chart Maker
(D) Data Mesh Diagram

**Oct/Nov 2025**

**64.** Which of the following correctly explains why the CMMI (Capability Maturity Model Integration) project was formed?
(A) Because the original CMM did not support project management software like MS-Project for various teams.
(B) Because CMM Level 5 was deemed unachievable by the Software Engineering Institute for small firms.
(C) Because applying multiple CMM models that were not integrated within an organization was costly in training and appraisals.
(D) Because the waterfall model completely replaced process maturity concepts in modern software design.

**May/June 2005**

**65.** Which of the following factors does not contribute to success in managing system projects?
(A) Reverting to an ad hoc process model during times of stress.
(B) Making the best of project team abilities.
(C) Assigning worthwhile jobs to team members.
(D) Providing opportunities to team members to use their abilities, advance, and develop their carriers.

**Oct/Nov 2016**

**66.** Which of the following is not an advantage of a Centralized Data Environment?
(A) Allowing each local unit to customize databases due to diverse usage and definitions.
(B) Consolidating and integrating data from all parts of the organization into one cohesive unit.
(C) Assuring that all data reflects the same time value for accurate reporting and analytics.
(D) Providing management with a clear view of the flow of data through the organization's network.

**May/June 2019**

**67.** Which of the following is not a characteristic or capability of a Group Decision Support System (GDSS)?
(A) Issue interpretation and consolidation of ideas.
(B) Access to decision making models and

Click Here to Buy book on Amazon

database management tools.
(C) Ensuring that all decisions are made strictly by a single top executive.
(D) Parallel communication and electronic recording.

**Oct/Nov 2011**

**68.** Consider the following elements related to Key Process Areas in CMM:
I. They identify a cluster of related activities that achieve a set of goals.
II. They reside at multiple maturity levels simultaneously.
III. The goals summarize the key practices of a key practice area.
IV. They are used to determine whether an organization has effectively implemented the key process area.
V. They are composed of Common Features.
Which of the above statement(s) is/are correct?
(A) I, II, IV, and V
(B) I, III, IV, and V
(C) II, III, IV, and V
(D) I, II, III, and V

**May/June 2007**

**69.** At which CMM maturity level does the primary focus shift from product quality to process quality, characterized by establishing process measures to initiate corrective actions?
(A) Level 2
(B) Level 4
(C) Level 3
(D) Level 5

**Oct/Nov 2022**

**70.** Which of the following statements regarding the rules of a PERT chart?
(A) The arrow length accurately scales the amount of time an activity requires for completion.
(B) A task can start even before the tasks it depends on have been completed by the team.
(C) The sequence and interconnections must give a true picture of the precedence of activities to be completed.
(D) PERT allows 'looping back' to accommodate iterative revisions during the development process.

**May/June 2018**

**71.** If a radical change takes place in a business strategy or operations, how does this impact a centralized database environment?
(A) The impact affects all areas because of their reliance on the central data pool, potentially causing a shift to a decentralized environment.
(B) The impact is isolated to the specific local department that initiated the change in strategy.
(C) The impact is mitigated by utilizing multiple independent semi-autonomous databases across units.
(D) The impact reduces data redundancy without affecting operations personnel or end-user functions.

**Oct/Nov 2015**

**72.** A project manager wants to monitor the progress of a project by identifying activities, the time they require, and their sequence, while specifically displaying the interdependence and precedence relationships of tasks. Which tool is most appropriate?
(A) Gantt Chart - Used for plotting project activities against a simple time frame for management.
(B) Program Evaluation and Review Technique (PERT)
(C) EPF Composer - Used for process management and standardizing various software development methods.
(D) Upper CASE tool - Used for requirements gathering and initial analysis during the planning stage.

**May/June 2024**

**73.** In the following question, a statement of Assertion (A) is followed by a statement of Reason (R):
Assertion (A): At the Initial level (Level 1) of CMM, software quality is highly predictable and independent of specific individuals.
Reason (R): Level 1 is characterized by a chaotic, ad hoc environment where few, if any, organized processes exist.
Select the correct answer:
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true,

Downloaded from www.pdf.tube

but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2017**

**74.** Consider the following components shown by a PERT chart:
I. The activities that must be completed before initiating a specific activity.
II. Inter-dependencies of the tasks.
III. The precise financial cost associated with each activity.
Which of the above statement(s) is/are correct?
(A) I and II
(B) II and III
(C) I and III
(D) I, II, and III

**May/June 2012**

**75.** Which of the following statements about SPOF is incorrect?
(A) It is a part of a system that, if it fails, will stop the entire system from working.
(B) SPOFs are undesirable in any system with a goal of high availability.
(C) Redundancy for all SPOFs ensures 24 x 7 availability of the data centre.
(D) Redundancy should be eliminated to isolate all SPOFs in a data centre.

**Oct/Nov 2008**

**76.** Which of the following incorrectly defines an aspect of Project Management?
(A) It is the process of planning, designing and implementing a computer system to meet specific goals.
(B) It is directed by a project manager who uses available resources to produce systems on time.
(C) It includes estimating resource requirements, scheduling tasks, and periodic evaluation of progress.
(D) It completely eliminates the need for contingency planning once the network is drawn.

**May/June 2023**

**77.** Match the CMM Maturity Levels in List I with their key characteristics in List II:
List I: Maturity Level
P. Level 1
Q. Level 2
R. Level 3
S. Level 5
List II: Key Characteristics
1. Peer reviews and codified standards.
2. Ad hoc, chaotic processes.
3. Evaluating new candidate processes and technologies.
4. Basic project management, dependent on individuals in stress.
(A) P-4, Q-2, R-3, S-1
(B) P-1, Q-3, R-2, S-4
(C) P-2, Q-1, R-4, S-3
(D) P-2, Q-4, R-1, S-3

**Oct/Nov 2006**

**78.** Consider the following steps for drawing a Gantt chart:
I. Determine the estimated time for each activity and obtain an agreement to proceed.
II. Identify the activities and tasks in the stage.
III. Plot activities on the Gantt chart, review and record the progress periodically.
IV. Determine the tasks for each activity and estimated completion times.
Which of the following represents the correct chronological sequence?
(A) II, IV, I, III
(B) I, II, IV, III
(C) II, I, IV, III
(D) IV, II, I, III

NODIA

**May/June 2020**

**79.** An organization has codified software development practices into a set of standards and procedures, provides training in these practices, and conducts peer reviews. The process belongs to the organization, and practices are not abandoned at times of stress. Which CMM maturity level has this organization achieved?
(A) Level 2: Repeatable Level
(B) Level 3: Defined Level
(C) Level 4: Managed Level
(D) Level 5: Optimizing Level

**Oct/Nov 2013**

**80.** Consider the following structural components of the CMM:
I. With the exception of the Initial Level, each level is composed of several key process areas (KPAs).
II. Each KPA is organized into five sections

called Common Features.
III. The Common Features specify the key practices that accomplish the goals of the key process area.
IV. The framework describes an evolutionary improvement path consisting of ten maturity levels.

Which of the above statement(s) is/are correct?
(A) I, II, and IV
(B) II, III, and IV
(C) I, II, and III
(D) I, III, and IV

**May/June 2010**

**81.** What is the most appropriate description of 'Management Awareness' in a centralized data environment?
(A) The requirement that management manually backs up data off site daily for disaster recovery purposes.
(B) The fragmentation of the global model leading to a loss of synergistic quality across departments.
(C) The clearer framework provided by data interaction and flow for understanding how various functions interact and affect the unit.
(D) The tendency to develop dialects within local data definitions that differ from the central standard.

**Oct/Nov 2009**

**82.** In a PERT chart, what is the conceptual meaning of an 'event'?
(A) A terminal achievement that has no duration and simply tells that an activity has ended or begun.
(B) A process that has a specific duration measured in days or weeks for the project timeline.
(C) An activity that can be 'looped back' to an earlier phase of the software development cycle.
(D) A horizontal bar representing the total project completion time in a simple management chart.

**May/June 2016**

**83.** What is an effective approach for a Project Manager to maintain a satisfied staff for strong project teams?
(A) Assigning them repetitive tasks to build routine efficiency and reduce training time for new hires.
(B) Minimizing communication to ensure they focus solely on coding and technical implementation tasks.
(C) Relying strictly on automated CASE tools to evaluate their performance and provide annual feedback.
(D) Improving job satisfaction by getting them interested in their jobs and recognizing their efforts spontaneously.

**Oct/Nov 2021**

**84.** How does the Capability Maturity Model primarily assist organizations on a global scale?
(A) By replacing all software engineers with automated CASE tools and AI-driven development systems.
(B) By standardizing proprietary hardware standards across competing organizations for better interoperability.
(C) By defining a scale for measuring process maturity, allowing accurate comparison of process capability and serving as a blueprint for improvement.
(D) By enforcing a decentralized data mesh strategy for all software development projects globally.

**May/June 2013**

**85.** What is the most appropriate description of the 'Activities Performed' common feature in CMM?
(A) It describes attributes that indicate whether implementation is lasting.
(B) It describes the institutionalization factors which make a process part of the culture.
(C) It describes the implementation activities of the key process area.
(D) It dictates the financial commitment required for process management.

**Oct/Nov 2024**

**86.** Identify the incorrect pair regarding the drawing steps and features of a Gantt chart:
(A) Left end of the bar - Shows the beginning of the task
(B) Horizontal bars - Show precedence relationship among the tasks
(C) Upper left of chart - Displays earlier tasks
(D) Lower right of chart - Displays later tasks

Click Here to Buy book on Amazon

May/June 2006

**87.** Consider the following statements regarding Data Centers:

I. A data center must connect to one or more communications networks and incorporate sufficient redundancy to guarantee round-the-clock connectivity.

II. A single point of failure (SPOF) is highly desirable in data centers to concentrate management control.

Which of the above statement(s) is/are correct?

(A) Only I
(B) Only II
(C) Both I and II
(D) Neither I nor II

Oct/Nov 2012

**88.** Which of the following is not considered a required quality of a Project Manager?

(A) Flexibility and adaptability to changing situations.
(B) Avoiding technical problems and delegating design details entirely to programmers.
(C) Ability to communicate and persuade people working on the project.
(D) Understanding the motivations and interests of members of the project.

May/June 2021

**89.** Which level of CMM is defined by using process measures to evaluate candidate new processes and determine the efficacy of introducing new technologies into the organization?

(A) Optimizing Level
(B) Defined Level
(C) Managed Level
(D) Repeatable Level

Oct/Nov 2005

**90.** Which of the following statements regarding the introduction of the Capability Maturity Model (CMM) is incorrect?

(A) It describes a path from a mature and disciplined process to an ad hoc, immature process.
(B) It was introduced by the Software Engineering Institute (SEI) at Carnegie Mellon University for assessment.
(C) It was introduced in the year 1987 to provide a framework for software process improvement globally.
(D) It was originally intended as a tool to evaluate the ability of government contractors to perform projects.

May/June 2017

**91.** In a decentralized database, users feel the database is 'their data' and take an active interest in its protection. Any flaw in database content can be readily traced to the group responsible. This scenario describes which specific advantage?

(A) Loss of Synergy
(B) User Confidence
(C) Lack of Central Control
(D) Data Integration

Oct/Nov 2023

**92.** Which of the following is not a factor considered under Site-related Risks for a data center?

(A) Heavy population in cities causing power overloads.
(B) Trees located where they could fall on necessary utility lines.
(C) The age of the building and compliance with electric safety codes.
(D) Ground impedance factors and soil types affecting proper grounding.

May/June 2009

**93.** Which of the following concepts is not associated with the thrust towards a Decentralized Data Environment?

(A) Functional specialization
(B) User proximity
(C) Universal data dialects unification
(D) Local differences in accounting practices

Oct/Nov 2019

**94.** Which of the following incorrectly describes a Tier 4 data center?

(A) It is fault-tolerant and provides the highest level of availability for enterprise-scale data centers.
(B) It allows for the occurrence of any unplanned activity while still maintaining operations for users.
(C) It is highly vulnerable to operational errors causing immediate system-wide outages.
(D) It features no single points of failure within its power and cooling infrastructure components.

NODIA

**May/June 2015**

**95.** Which emerging trend describes a movement to bring the web back to its original vision of a neutral network where everyone can participate without depending on any single 'central' organization?
(A) Data Warehouse - A centralized repository for storing large volumes of historical analytical data.
(B) Web 3.0 (Decentralized Web)
(C) Tier-IV Data Centre - A fault-tolerant facility designed for maximum availability and redundancy.
(D) Central Repository CASE - A tool for managing system specifications and requirements documents.

**Oct/Nov 2007**

**96.** Which of the following is not a redundancy measure provided for communication lines between branches and the DC & DR?
(A) MPLS Links
(B) Disconnecting the city Network Aggregation Point from the DR
(C) 3G/4G connections
(D) Alternate lease lines from another telecom operator

**May/June 2025**

**97.** Consider the following statements regarding the Decentralized Data Environment:
I. It consists of multiple databases each serving some segment, often involving semi-independent organizational units.
II. Linkages between systems may involve sharing common data or uploading/ downloading reference data from a common source.
Which of the above statement(s) is/are correct?
(A) Only I
(B) Only II
(C) Both I and II
(D) Neither I nor II

**Oct/Nov 2014**

**98.** Which of the following incorrectly states an advantage of the Data Mesh approach?
(A) It provides a connectivity layer that requires costly data transfers and residency concerns.
(B) Data is viewed as a product in the distributed architecture for better domain-specific management.
(C) It delegates dataset ownership from the central infrastructure team to individual business domains.
(D) It steers enterprises toward real-time decision-making by closing the time and space gap in data.

**May/June 2011**

**99.** Consider the following business projections evaluated during facility selection:
I. The probability of earthquakes in the region.
II. Whether the facility meets the operating requirements for the first five years.
III. The grounding system soil humidity.
IV. The co-location capabilities of rival telecommunication carriers.
Which of the above must management review to meet short-term and long-term size requirements?
(A) Only I
(B) Only II
(C) I and III
(D) II and IV

**Oct/Nov 2020**

**100.** What is the most appropriate reason why Corporate-Level Reporting is challenging in a decentralized data environment?
(A) Data integration ensures all units use exact identical formats without compromise for all reporting.
(B) Centralized management has total control over data sharing protocols across all functional departments.
(C) Dispersion of data and local definitions make aggregate, cross-unit reports more difficult to prepare.
(D) SPOFs automatically consolidate data to the central mainframe for streamlined corporate-level analysis.

**May/June 2008**

**101.** Match the Information System concepts in List I with their specific characteristics in List II:
List I: Concept
P. Capability Maturity Model (CMM)
Q. PERT Chart
R. Groupware
S. Decentralized Database
List II: Characteristics
1. Emphasizes determining the critical path and precedence relationships without

Downloaded from www.pdf.tube

looping back.
2. Characterized by user proximity and potential data redundancy.
3. Designed to describe an evolutionary improvement path for software processes.
4. Enables sharing of information for synchronous or asynchronous collaboration.

(A) P-3, Q-1, R-4, S-2
(B) P-1, Q-2, R-3, S-4
(C) P-4, Q-3, R-1, S-2
(D) P-2, Q-4, R-2, S-1

**Oct/Nov 2018**

**102.** Which of the following correctly identifies an advantage of 'User Proximity' in a decentralized database?

(A) The database has a narrower audience and tends to serve the individual user better than a centralized database.
(B) The data administrator has more variables to coordinate when assigning responsibility for the systems.
(C) Data ownership is deliberately kept ambiguous to encourage global collaboration between various groups.
(D) The database relies entirely on the corporate parent's un-synchronized data models for its structure.

**May/June 2022**

**103.** In the following question, a statement of Assertion (A) is followed by a statement of Reason (R):

Assertion (A): Adding redundant utility feeds and carrier lines helps reduce the likelihood of the power going down.

Reason (R): Redundant communication lines should be mandatory for those sites whose business relies on availability.

Select the correct answer:

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2010**

**104.** Which of the following statements regarding Bitcoin and Block-chain technology is correct?

(A) Block-chain technology relies entirely on proprietary legacy mainframes for processing all transactions.
(B) The concept behind cyber currency completely prohibits the use of a centralized registry for members.
(C) Block-chain completely replaces the need for NEFT in all Indian banks for domestic fund transfers.
(D) Block-chain is essentially a distributed database or ledger where every event is registered as an unalterable block.

**May/June 2014**

**105.** Match the components of a Disaster Recovery setup in List I with their descriptions in List II:

List I: Component
P. Data Centre (DC)
Q. Disaster Recovery site (DR site)
R. Redundancy at every stage
S. NAP

List II: Description
1. Setup in a different seismic zone to prevent complete stand-still.
2. Network Aggregation Point connected to both DC and DR.
3. Provided in the form of MPLS Links, 3G/4G connections, or alternate lease lines.
4. The location where the entire data of an organization primarily resides.

(A) P-1, Q-4, R-2, S-3
(B) P-4, Q-3, R-1, S-2
(C) P-4, Q-1, R-3, S-2
(D) P-2, Q-1, R-4, S-3

NODIA

**Oct/Nov 2025**

**106.** Consider the following statements regarding downloading and uploading in a decentralized environment:

I. Downloading involves the extraction of data from a central database and normally reformatting it into a usable form.
II. Uploading involves the extraction of data from receiving systems to a separate external parent company without reformatting.
III. In each case, rules on data modification and data sharing must be carefully documented due to indirect links.

Which of the above statement(s) is/are correct?

(A) I and II
(B) II and III
(C) I and III

(D) I, II, and III

May/June 2005

**107.** Consider the following features regarding a Tier III data center:

I. It is concurrently maintainable.
II. It offers N+1 availability in terms of redundancy.
III. It allows planned maintenance of power and cooling systems without disrupting computer hardware operation.
IV. Unplanned activity such as spontaneous failures can still cause an outage.
V. It is completely fault-tolerant.

Which of the above statement(s) accurately describes Tier III?

(A) I, II, III, and IV
(B) I, II, III, and V
(C) II, III, IV, and V
(D) I, III, IV, and V

Oct/Nov 2016

**108.** In the following question, a statement of Assertion (A) is followed by a statement of Reason (R):

Assertion (A): The coordination of decentralized databases and their interaction is a difficult task.
Reason (R): Decentralized databases are the property of corporate management, who impose strict centralized data entities and relationships.
Select the correct answer:

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2019

**109.** What is the most appropriate reason why a data center is not recommended to be located under a kitchen or in a basement?

(A) Due to Economic risks such as high construction costs and state-level tax incentive structures.
(B) Due to Geographic risks such as tornadoes, earthquakes, or seasonal flooding in the regional area.
(C) Due to the unavailability of skilled labour in basement environments for technical data management.
(D) Due to Building risks involving threats posed by other applications and multi-tenant neighbours.

Oct/Nov 2011

**110.** Consider the following statements about Data Mesh:

I. It is a new approach based on a modern, distributed architecture for analytical data management.
II. It distributes data ownership to domain-specific teams that manage and serve data as a product.
III. It requires users to first transport data to a data lake or data warehouse before accessing it.

Which of the above statement(s) is/are correct?

(A) I and II
(B) II and III
(C) I and III
(D) I, II, and III

May/June 2007

**111.** Consider the following components ensuring continuity of business and services:

I. Disaster Recovery Site (DRS) in a different seismic zone.
II. MPLS Links and Wireless connectivity.
III. Network Aggregation Point (NAP) connected to both DC & DR.
IV. Placing all backup servers in the exact same facility as the primary DC.

Which of the above statement(s) represents a correct setup for a proper DRS?

(A) I, II, and III
(B) I, II, and IV
(C) II, III, and IV
(D) I, III, and IV

Oct/Nov 2022

**112.** Match the attributes in List I to the Data Environments in List II:

List I: Attribute
P. Data Redundancy
Q. Data Integration
R. Corporate-Level Reporting difficulty
S. Management Awareness and unified flow

List II: Data Environment Type
1. Centralized Data Environment advantage
2. Decentralized Data Environment disadvantage

Click Here to Buy book on Amazon

the maintenance burden on internal departments. This trend allows businesses to implement proven solutions quickly while minimizing the risks and resource requirements associated with building complex software systems from the ground up.

**9.** (B) To accelerate the development of the project and help uncover flaws before moving ahead with the next stage.
Computer-Aided Software Engineering tools provide significant advantages by accelerating the development lifecycle through automation and improved coordination. These tools help identify logic flaws and inconsistencies early in the process, preventing expensive errors in later stages. By streamlining analysis and design, CASE tools enhance the overall quality and reliability of the software while reducing the total time required for project completion.

**10.** (C) P-2, Q-4, R-1, S-3
Programming languages are categorized by generations and specific characteristics suited for different tasks. Assembly language is a second-generation language providing low-level hardware control. FORTRAN is a third-generation language designed for scientific and engineering applications. SQL functions as a fourth-generation language for database queries, while Oracle Forms represents a 4GL tool specifically utilized for creating complex software development applications and user interfaces.

**11.** (D) Interactive or real time mode
Interactive or real-time processing ensures that the master file is updated immediately as transactions occur, maintaining the most current information. This mode is critical for applications like banking or reservation systems where accuracy and up-to-the-minute data are essential for operations. Unlike batch processing, which groups transactions for periodic updates, real-time mode provides instant feedback and reflects the current state of affairs.

**12.** (C) II, IV, V, III, I
The Software Development Life Cycle follows a logical sequence beginning with planning and analysis to define requirements. This is followed by design and development, where the system architecture is created. After development, the system undergoes testing and acceptance to ensure quality standards. Once approved, the implementation phase occurs, followed by ongoing operation and maintenance to support the system during its lifecycle.

**13.** (A) I, II, and III
Effective deployment strategies include parallel deployment, where old and new systems run simultaneously to ensure reliability, and phased deployment, which introduces the system in stages. Pilot deployment tests the entire system within a specific organizational subset before a full-scale rollout. These methods minimize operational risks, unlike direct cutover where the old system is immediately replaced, potentially leading to significant downtime if issues arise.

**14.** (C) I and III
The Internet relies on open standards like TCP/IP, which are developed through collaborative committees to ensure interoperability across different platforms and vendors. These standards are publicly available and not controlled by a single entity. In contrast, proprietary standards are owned by specific companies and often restrict compatibility, making open standards essential for the global connectivity and neutral participation characteristic of the modern web.

**15.** (D) Prototyping Tools
Prototyping tools are utilized during the design phase to create an initial look and feel of a product, simulating user interfaces without requiring full hardware integration. These tools allow users to interact with a model of the system, providing valuable feedback before the actual coding begins. This iterative process helps refine requirements, identify potential usability issues, and ensure the final software meets expectations.

**16.** (A) Information System
An information system is a coordinated set of components that work together to collect, process, and distribute data to produce meaningful output. It encompasses hardware, software, data, people, and procedures designed to support organizational decision-making and control. By transforming raw inputs into valuable information, these systems enable businesses to manage operations efficiently and achieve strategic goals through structured processing and storage mechanisms.

NODIA

sites.
III. The availability of skilled labour in the region.
IV. Type of area (urban vs rural) impacting power consumption overloads directly.
Which of the above are categorized strictly under Economic Risks?
(A) I, II, and III
(B) II, III, and IV
(C) I, III, and IV
(D) I, II, and IV

**Oct/Nov 2006**

**120.** Consider the following statements regarding the application of block-chain in banking:
I. It can be used in trade finance to mitigate the risk of fraud, such as multiple discounting of the same invoice.
II. All subsequent events related to a loan can be put on the "block" so members can take informed decisions.
Which of the above statement(s) is/are correct?
(A) Only I
(B) Only II
(C) Both I and II
(D) Neither I nor II

**May/June 2020**

**121.** A bank's data center is located in a multi-tenant building where heavy industrial machinery runs frequently. What specific building risk is caused by the heavy power draw of this equipment?
(A) Creation of alternate lease lines to provide redundancy for the main communication network.
(B) Ground impedance failures due to high humidity levels and poor soil quality in the region.
(C) A shift from a centralized to a decentralized data mesh architecture across the entire firm.
(D) Sags within the building and for surrounding miles

**Oct/Nov 2013**

**122.** While acquiring software, an organization ensures the new application integrates smoothly with current network protocols and OS, processes inputs swiftly, and offers robust technical support. Which SDLC evaluation factor is being primarily tested here?
(A) Defining system performance criteria in the planning phase
(B) Setting proprietary communication standards
(C) Evaluating compatibility, functionality, speed, and technical support
(D) Conducting a feasibility study for hardware design

**May/June 2010**

**123.** A bank configures its branches to link to the primary data center and the disaster recovery site using primary leased lines. To prevent a complete loss of service if the primary provider fails, what specific topology is established?
(A) The Network Aggregation Point (NAP) is physically relocated to a Level 1 CMM organization facility.
(B) The branches switch to batch updating mode exclusively on local terminals for all daily transactions.
(C) The city Network Aggregation Point (NAP) is connected to both DC & DR with alternate lease lines from another telecom operator acting as a backup.
(D) The bank relies solely on a single point of failure (SPOF) to streamline all its internal operations.

**Oct/Nov 2009**

**124.** Which of the following is not a factor considered to ensure the stability of grounding and wiring in a Site-related risk assessment?
(A) The tax incentives offered by the state
(B) Weather and animals on lines
(C) The use of underground wiring
(D) Ground impedance factors, soil types, and humidity

NODIA

**May/June 2016**

**125.** In the following question, a statement of Assertion (A) is followed by a statement of Reason (R):
Assertion (A): Establishing a Disaster Recovery Site (DR site) in a different seismic zone mitigates concentration risk.
Reason (R): In the event of something happening at the primary DC, the DR site allows the other facility to take over, ensuring continuity of business.
Select the correct answer:
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of

(A) P-1, Q-2, R-1, S-2
(B) P-2, Q-1, R-2, S-1
(C) P-1, Q-1, R-2, S-2
(D) P-2, Q-2, R-1, S-1

**May/June 2018**

**113.** What is the most appropriate consequence when the global informational model is fragmented in a decentralized environment?
(A) Increased Data Integration
(B) Complete elimination of Data Redundancy
(C) Loss of Synergy
(D) Transition to Tier 4 Redundancy

**Oct/Nov 2015**

**114.** Which of the following statements regarding Tiers of Redundancy of a Data Centre is correct?
(A) Tier III data centers are completely fault tolerant and allow for the occurrence of any unplanned activity.
(B) A Tier III data center is concurrently maintainable, allowing for planned maintenance without disrupting operations.
(C) Tier 4 facilities have single points of failure which are monitored by a central management team.
(D) Most banks have adopted Tier 4 redundancy due to zero cost constraints and minimal technical needs.

**May/June 2024**

**115.** Match the categories of risks in Data Centers in List I with their corresponding examples or factors in List II:
List I: Risk Category
P. Geographic and Regional Risks
Q. Site-related Risks
R. Building Risks
S. Economic Risks
List II: Example or Factor
1. Types of loads running, sags, elevators, and location within a facility.
2. Tax incentives, utility rate structure, and land costs.
3. Tornadoes, earthquakes, floods, and lightning.
4. Heavy populations causing power overloads, rural areas with trees near lines.
(A) P-4, Q-3, R-2, S-1
(B) P-1, Q-2, R-3, S-4
(C) P-3, Q-1, R-4, S-2
(D) P-3, Q-4, R-1, S-2

**Oct/Nov 2017**

**116.** Which of the following statements incorrectly describes 'Local Differences' in a decentralized database?
(A) Opportunities for compromise are limited by diverse data requirements at the local level.
(B) Each local unit is essentially a separate organization with little in common with other units.
(C) Distinct differences in accounting practices can make decentralization the correct choice.
(D) Data is fed downwards from senior parent management to conform to strict central standards.

**May/June 2012**

**117.** In the following question, a statement of Assertion (A) is followed by a statement of Reason (R):
Assertion (A): Financial institutions have gradually started moving towards Tier-IV Data Centres.
Reason (R): The criticality has been increasing on account of 24 x 7 services being extended.
Select the correct answer:
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2008**

**118.** In which condition is the same piece of data held in two separate places, often resulting in discrepancies, inaccuracies, and demanding increased management control in a decentralized environment?
(A) Data Mesh
(B) Data Integration
(C) Web 3.0
(D) Data Redundancy

**May/June 2023**

**119.** Consider the following factors evaluated before selecting a new site:
I. Tax and other incentives.
II. Overall operating costs relative to other

Downloaded from www.pdf.tube

# ANSWERS

1. (D) Costs are projected for the first time during testing rather than the design phase.
In the Software Development Life Cycle, cost projections and feasibility studies occur early during the planning and analysis stage to determine project viability. The design and development stage focuses on creating system elements like screens and reports while selecting technical tools. Waiting until the testing phase to estimate costs is an ineffective practice that risks project failure and budget overruns.

2. (C) Acquisition projects replace the SDLC design and development phases with a bid solicitation process.
Software acquisition involves obtaining pre-built systems or hiring external vendors rather than building solutions in-house. While development projects follow the standard design and development phases, acquisition projects substitute these stages with a formal bid solicitation process to select vendors. This approach requires management to define specific functional and security requirements to ensure the chosen product meets the organization's needs.

3. (C) Problem Solving
Problem solving is a fundamental process where individuals identify a discrepancy between the current reality and a preferred future state. This involves structuring a sequence of choices to bridge the gap and achieve organizational goals. It differs from system analysis by focusing on the broader decision-making framework required to resolve issues and improve overall functional performance within a business context.

4. (C) Configuration Management Tools - Fossil, Git, Accu REV
Configuration management tools are essential for managing different versions of software and controlling changes during the development process. Examples like Fossil, Git, and Accu REV allow teams to track modifications, maintain code integrity, and collaborate effectively. These tools automate file management and ensure that developers are working on the most recent and accurate iterations of the system software.

5. (B) Only II
Distributed networks utilize departmental mini-computers to process applications locally while maintaining periodic communication with a central mainframe for data synchronization. This contrasts with centralized networks where dumb terminals lack processing power and rely entirely on the host mainframe for calculations. Distributed systems offer greater flexibility and resilience by allowing individual units to handle specific operational tasks independently of the central server.

6. (C) Assertion (A) is true, but Reason (R) is false.
Quality Assurance tools are designed to ensure that software development adheres to established organizational standards and quality metrics. While these tools facilitate monitoring and error prevention, they are not limited solely to post-delivery logging and root cause analysis. Effective quality assurance involves a proactive approach throughout the entire development lifecycle, rather than just focusing on modifications after the software is deployed.

7. (B) Data
Data consists of raw facts, figures, and text collected during business operations that lack context or specific meaning on their own. Until processed and analyzed, these observations do not provide significant value to the organization. Once data is organized and interpreted to provide insights for decision-making, it transforms into information, which is a critical asset for strategic planning and management.

8. (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Organizations increasingly prefer purchasing software packages over custom development because they are more cost-effective and immediately available for deployment. These packages are supported by the vendor, reducing

NODIA

provide comprehensive support across all stages. A central repository serves as a critical data dictionary, storing requirement documents and project specifications to ensure consistency and facilitate collaboration among the development team.

**25.** (B) Testing & Acceptance
During the testing and acceptance stage, the development team identifies and fixes product defects to ensure the software meets the quality standards defined in the requirements specification. This phase involves rigorous evaluation of the system's functionality and performance. Successful completion signifies that the product is ready for deployment. This process is distinct from the operation and maintenance stage, which occurs after the software is live.

**26.** (D) Hardware, Software, Data, People, and Procedures
An information system comprises five essential components that work together to manage data and support organizational functions. Hardware includes the physical equipment, while software provides the instructions for processing. Data represents the raw information being managed. People are the users and professionals who interact with the system, and procedures are the rules or guidelines that govern how the system is used to achieve objectives.

**27.** (A) Providing live previews of web pages
Change control tools are designed to automate file and code management while enforcing an organization's change policies. They ensure that modifications to software are tracked, authorized, and documented to maintain system integrity. While these tools are vital for version control and configuration management, they typically do not include features for providing live previews of web pages, which is more commonly associated with web development environments.

**28.** (A) To coordinate group programmers, manage large projects, and analyze programs.
Utilizing CASE tools within a development environment allows organizations to efficiently coordinate large teams of programmers and manage complex projects. these tools provide sophisticated features for analyzing programs, detecting errors, and maintaining consistency across different development phases. By automating routine tasks and facilitating better communication, CASE tools help ensure that software projects are completed on time, within budget, and according to established quality standards.

**29.** (C) Central Repository
A central repository is a fundamental component of integrated CASE tools, providing a single location for storing product specifications, requirement documents, and data dictionaries. This ensures that all team members have access to consistent, up-to-date information throughout the development lifecycle. By centralizing these assets, organizations can improve collaboration, reduce data redundancy, and maintain the integrity of project documentation, which is essential for successful system delivery.

**30.** (D) Implementation
In software acquisition projects, the implementation stage involves evaluating potential products based on criteria such as hardware compatibility, speed, error handling, and maintenance costs. Management assesses whether the software meets the defined functional and security requirements before final selection and deployment. This phase ensures that the acquired solution integrates effectively with existing infrastructure and provides the necessary capabilities to support the institution's branch operations.

**31.** (C) Assertion (A) is true, but Reason (R) is false.
Top management primarily requires strategic information concerning the external environment to make long-term decisions and plan for the organization's future. They focus on broad trends rather than detailed operational data about daily branch activities. Detailed reports are more appropriate for lower-level managers who supervise routine procedures. Therefore, while the need for external information is paramount for senior executives, the focus on internal operational details is misplaced.

**32.** (B) A rigid system structure that prevents adaptation to changing conditions over time.
Decision Support Systems are characterized by their flexibility and ability to adapt to changing conditions over time. A rigid structure would

Click Here to Buy book on Amazon

17. (B) I, II, III, and IV
CASE tools offer various functionalities to support development, including diagram tools for graphical representation and process modelling for selecting software models. Project management tools assist with cost estimation and information sharing, while analysis tools automatically detect inconsistencies and data redundancies. Documentation tools are also vital, as they generate necessary manuals for both in-house professionals and end-users, ensuring comprehensive knowledge transfer across the organization.

18. (A) Prolog
Third-generation languages, such as Java, Pascal, and Python, are high-level programming languages that are easier for humans to read and write compared to machine code. They utilize compilers or interpreters to translate instructions into executable formats. Prolog is distinct because it is categorized as a fifth-generation language, focusing on logic programming and artificial intelligence rather than the procedural or object-oriented approaches common in 3GLs.

19. (D) The risks associated with using general business purpose software are typically higher than those for financial applications.
Acquiring software involves soliciting bids through invitations-to-tender for hardware or requests-for-proposals for off-the-shelf applications. Financial software requires more stringent evaluation due to its critical nature and the high risks associated with data integrity and security. Conversely, general business software typically presents lower risks, although compatibility and functionality must still be carefully assessed to ensure the chosen solution effectively supports organizational operations.

20. (A) P-3, Q-1, R-4, S-2
Different software development models cater to specific project needs. The waterfall model involves specifying the entire system upfront before development begins. In the spiral model, users specify parts of the system incrementally. Prototyping involves creating a simple version for user feedback and repeated modification. Software packages offer a less expensive, immediately available alternative that is supported by vendors, bypassing the need for custom internal development.

NODIA

21. (C) Design Tools - Checking for data redundancies and erroneous omissions
Analysis tools are specifically designed to check for data redundancies, inconsistencies, and erroneous omissions within a system model. Design tools, however, focus on creating the structural architecture, user interfaces, and report layouts of the software. While related, these functions are distinct; analysis ensures the logical integrity of the requirements, whereas design translates those requirements into technical specifications for the final product development.

22. (B) Organizing the project team, gathering business requirements, and defining system performance criteria
The planning and analysis stage of the software development life cycle involves defining the core problem and establishing a project team. Key activities include conducting feasibility studies and gathering detailed business requirements from stakeholders. Additionally, managers must define system performance criteria to ensure the final product meets organizational needs. This foundational stage sets the scope and objectives for all subsequent design and implementation efforts.

23. (D) UNIX/LINUX - Provides robust support for communication tasks and distributed computing
UNIX and LINUX operating systems are renowned for providing robust support for communication tasks and distributed computing environments. They offer powerful networking capabilities and multitasking features essential for enterprise-level server management. This contrasts with other systems like Macintosh, which historically focused on high-end graphics and multimedia. Understanding these strengths helps organizations select the most appropriate platform to host their critical applications and manage complex network infrastructures.

24. (D) P-4, Q-3, R-1, S-2
CASE tools are categorized based on the life cycle stages they support. Upper CASE tools are used during planning, analysis, and design, while Lower CASE tools assist with implementation, testing, and maintenance. Integrated CASE tools

Assertion (A).

(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).

(C) Assertion (A) is true, but Reason (R) is false.

(D) Assertion (A) is false, but Reason (R) is true.

www.nodia.in

Downloaded from www.pdf.tube

prevent a DSS from effectively supporting decision-making for semi-structured and unstructured problems. These systems feature integrated subsystems that allow managers to retrieve and manipulate information along broad functional lines. Furthermore, they are designed to be adaptive, enabling users to refine models as new information becomes available.

**33.** (B) TPS with interactive updating
An airline reservation system is a classic example of a Transaction Processing System that utilizes interactive or real-time updating. This ensures that seat availability is immediately adjusted as bookings are confirmed, preventing overbooking and providing accurate information to all users. Unlike batch processing, which groups transactions for later updates, interactive mode processes each event individually and immediately, which is essential for time-sensitive operations in competitive industries.

**34.** (D) Software that helps groups of people work together more efficiently and effectively by enabling collaborative computing.
Groupware refers to a category of software designed to help groups of people work together more effectively by enabling collaborative computing. It facilitates communication, coordination, and information sharing among team members, regardless of their physical location. This software can support both synchronous interactions, like video conferencing, and asynchronous activities, such as e-mail and shared calendars, ultimately enhancing productivity and collective decision-making within an organization.

**35.** (B) I and III
Strategic information is defined by its long-term nature and its focus on helping senior management plan the organization's future. It often includes simulated "what if" scenarios and data regarding competitive actions and the availability of external resources. Unlike operational information, which is descriptive and historical, strategic information is predictive and oriented toward identifying opportunities and threats in the external environment to achieve long-range goals.

**36.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
A Group Decision Support System provides automated tools to enter, record, and build upon the ideas of team members during collaborative sessions. Its capabilities include alternative generation, issue interpretation, and anonymous recording, which help eliminate barriers to effective group communication. By providing a structured environment for brainstorming and evaluation, GDSS enables groups to reach consensus and make more informed decisions while ensuring that all contributions are captured.

**37.** (A) TPS, MIS, and DSS
Information systems are generally classified into three major types based on the level of management they support and the nature of the problems they address. Transaction Processing Systems handle routine daily activities at the operational level. Management Information Systems provide structured reports for middle management control. Decision Support Systems offer interactive analytical tools to help managers solve semi-structured and unstructured problems using mathematical models and data.

**38.** (B) I, II, IV, and V
Decision Support Systems feature a broad-based approach to supporting management and utilize a human/machine interface where the user retains ultimate control. They incorporate appropriate mathematical and statistical models and provide interactive query capabilities for on-demand information retrieval. While they support semi-structured and unstructured decisions, they are not limited to highly structured problems, which are more typically handled by conventional transaction processing and management information systems.

**39.** (D) EIS
Executive Information Systems are specialized tools designed to provide senior managers with immediate access to information critical for accomplishing strategic objectives. These systems present multidimensional data according to the executive's personal preferences, often combining internal operational summaries with external market intelligence. EIS features easy-to-use

NODIA

interfaces and powerful visualization capabilities, allowing leaders to monitor performance trends and identify potential problems that require high-level intervention and strategic planning.

**40.** (D) It assists top management in strategic decisions characterized by a great deal of uncertainty.
Operational information is primarily used at the lowest level of decision-making to manage routine, daily tasks. It allows line managers to measure performance against specific objectives and provides feedback to keep higher management informed of results. However, it does not assist top management with strategic decisions characterized by high uncertainty. Strategic decisions require broad, predictive information rather than the detailed, structured, and repetitive data found in operational reports.

**41.** (B) Training decision makers to deal with disaster situations or high-risk situations.
Group Decision Support Systems are often utilized in specialized training environments to help decision-makers handle disaster or high-risk situations. By simulating complex scenarios, GDSS allows teams to practice collaboration, evaluate alternatives, and make critical decisions in a controlled setting. This application leverages the system's ability to facilitate communication and consensus-building, ensuring that participants develop the skills necessary to respond effectively to real-world challenges and emergencies.

**42.** (C) A DSS provides support for semi-structured decisions using highly interactive analytical models, whereas an MIS helps users identify problems.
The fundamental difference between a Decision Support System and a Management Information System lies in the nature of the support they provide. While an MIS typically summarizes data and provides structured reports to help users identify problems, a DSS offers highly interactive analytical models to support semi-structured decision-making. DSS enables users to perform complex "what-if" analyses and manipulate data directly, providing a deeper level of insight for non-routine management challenges.

**43.** (C) Assertion (A) is true, but Reason (R) is false.
In a Decision Support System, the use of CRT terminals allows the decision-maker to manipulate and present data through an interactive human/machine dialogue. This interface is designed so that the human retains control over the decision-making process at all times. The machine serves as a tool to enhance the executive's skills and judgment, rather than replacing the human or forcing them to surrender control to automated algorithms or models.

**44.** (D) Because professional judgment and insight are critical in decision making.
Decision Support Systems are designed to augment an executive's skills because professional judgment and personal insight remain essential for effective decision-making. While the system can process complex mathematical models and organize large volumes of data, it cannot replicate the human experience and intuition required to navigate semi-structured or unstructured problems. The goal is to provide a powerful tool that helps the manager evaluate alternatives and make more informed choices.

**45.** (C) Group Decision Support System (GDSS)
A Group Decision Support System utilizes advanced presentation devices and specialized software to facilitate collaborative problem-solving. It provides features for anonymously recording ideas and calculating the weights of various decision alternatives, which helps reduce groupthink and encourages participation. By providing a structured framework for brainstorming and evaluation, GDSS enables committees to manage complex information and reach more objective and well-reasoned conclusions during organizational meetings and workshops.

**46.** (B) Only II
Transaction Processing Systems often utilize batch updates to group similar transactions together, allowing for more efficient use of computer and network resources. While some tasks are processed in real time, payroll is a typical example of a process generally handled in batch mode. Batch processing is suitable for non-urgent tasks where periodic updates are sufficient, whereas real-time mode is necessary

Click Here to Buy book on Amazon

for time-sensitive operations like credit card processing or inventory management.

**47.** (B) Everyone's Information Systems and Enterprise Information Systems
As Executive Information Systems have become more accessible and widely used across organizations, they are increasingly referred to as Enterprise Information Systems or "Everyone's" Information Systems. This shift reflects their growing utility for a broader range of managers, analysts, and knowledge workers beyond just top-level executives. These systems now serve as comprehensive platforms for data visualization and strategic analysis, providing valuable insights to various functional departments throughout the entire enterprise.

**48.** (B) It covers relatively short periods, not greater than 12 months, and is used to implement strategic plans at the functional levels.
Tactical information is used by middle management to implement strategic plans at functional levels. It typically covers relatively short timeframes, generally not exceeding twelve months. This type of information is essential for allocating resources, monitoring progress, and ensuring that departmental activities align with the organization's broader long-term goals. Unlike operational information, which deals with daily tasks, tactical information focuses on the coordination and control of major business functions over a medium-term horizon.

**49.** (A) Integrated subsystems process data for use along traditional, narrow departmental lines.
Integrated subsystems within a Decision Support System are designed to process data along broad functional lines rather than traditional, narrow departmental boundaries. This integration allows managers to retrieve and manipulate information that transcends isolated units, providing a more comprehensive view of the organization. By facilitating cross-functional data access, these subsystems support more effective decision-making that considers the interconnected nature of various business activities and their impact on overall organizational performance.

**50.** (A) I and II
A Decision Support System consists of several key components, including a Database Management System that integrates internal data from TPS and MIS with relevant external information. The Model Management System stores various analytical models used for financial forecasting and demand analysis. Support Tools are also included to facilitate user interaction; however, they are specifically designed to enable highly interactive processing rather than restricting users to batch-mode operations, ensuring flexible decision support.

**51.** (D) It provides capabilities for summarizing, aggregating and collecting results, ranking opinions, and prioritizing tasks.
Group Decision Support System software provides specialized capabilities that go beyond individual workstation functions to facilitate collective work. It includes tools for summarizing and aggregating results from group sessions, as well as features for ranking opinions and prioritizing tasks anonymously. These functions help teams manage diverse perspectives, build consensus, and reach more effective decisions by providing a structured and efficient environment for collaboration and information exchange during group meetings.

**52.** (D) P-3, Q-1, R-2
Informational needs vary significantly across management levels. Top management requires overall reports that are fundamentally planning-oriented to guide the organization's long-term strategy. Middle management needs comprehensive reports that balance planning and control to manage functional departments. Lower management relies on detailed, control-oriented reports to oversee routine daily operations and ensure that specific tasks are completed efficiently and according to established standards. This hierarchy ensures appropriate data for different decision-making roles.

**53.** (C) Different kinds of decision making require differing but overlapping informational requirements based on the level of the decision maker.
In practical business situations, the distinctions between categories of managerial decision-making are often blurred because different types of decisions have overlapping informational requirements. A single decision-maker may need a mix of operational, tactical, and strategic

Downloaded from www.pdf.tube

making among multiple stakeholders, rather than centralizing authority in a single executive. Its capabilities include issue interpretation, alternative generation, and providing access to mathematical models and database tools. By enabling parallel communication and anonymous recording, GDSS helps groups overcome social pressures and ensures that all perspectives are considered, leading to more comprehensive and consensus-based outcomes that benefit the entire organization.

**68.** (B) I, III, IV, and V
Key Process Areas in the CMM identify clusters of related activities that achieve specific goals. These goals summarize the key practices and are used to determine whether an organization has effectively implemented a KPA. Each KPA consists of common features that describe implementation and institutionalization factors. Importantly, KPAs are specific to a single maturity level and do not reside at multiple levels simultaneously, as they represent the evolutionary steps in process maturity.

**69.** (B) Level 4
At the Managed Level (Level 4) of the Capability Maturity Model, the primary focus of the organization shifts from product quality to process quality. This transition is characterized by establishing quantitative process measures to monitor performance and initiate corrective actions. By collecting and analyzing detailed data about the development process, organizations can predict trends and ensure that software quality remains within acceptable limits, leading to more predictable outcomes and a deeper understanding of process capability.

**70.** (C) The sequence and interconnections must give a true picture of the precedence of activities to be completed.
In a PERT chart, the sequence and interconnections of activities must accurately reflect their precedence and dependencies. This ensures that the network provides a true picture of how tasks must be completed. Unlike Gantt charts, arrow length in PERT does not scale with time, and tasks cannot start until their prerequisites are finished. Furthermore, PERT is a one-way flow diagram that does not allow for "looping back" to earlier stages, maintaining a clear path toward completion.

**71.** (A) The impact affects all areas because of their reliance on the central data pool, potentially causing a shift to a decentralized environment.
In a centralized database environment, all organizational units rely on a single, shared data pool. Consequently, any radical change in business strategy or operations has a widespread impact across all areas of the firm. This high degree of interdependence means that modifications to central data structures or policies require careful coordination to avoid disrupting multiple departments. If the centralized model becomes too rigid to accommodate local needs, the organization might eventually consider shifting toward decentralization.

**72.** (B) Program Evaluation and Review Technique (PERT)
The Program Evaluation and Review Technique is the most appropriate tool for monitoring project progress while displaying complex interdependence and precedence relationships among tasks. PERT identifies the sequence of activities and the time required for each, allowing managers to determine the critical path. This differs from a Gantt chart, which primarily focuses on plotting tasks against a simple timeline without highlighting the intricate dependencies that can impact the overall project schedule and delivery.

**73.** (D) Assertion (A) is false, but Reason (R) is true.
At the Initial Level (Level 1) of the Capability Maturity Model, software processes are typically chaotic and ad hoc, with very few organized procedures in place. Consequently, project success is highly unpredictable and depends heavily on the individual efforts of talented staff rather than organizational capability. The assertion that quality is predictable at this level is false, as the lack of a stable process framework makes it difficult to replicate successes or manage risks effectively across different projects.

**74.** (A) I and II
A PERT chart is designed to show the activities that must be completed before a specific task can initiate, as well as the overall inter-dependencies between various project elements. It focuses

NODIA

branches, enabling local managers to solve complex problems independently. This trend shifts decision-making power closer to the operational level while maintaining data integrity through sophisticated DBMS technology, ultimately improving organizational agility and responsiveness in competitive markets.

**61.** (C) It is the longest path through the network where no task can be held up without delaying the completion of the project.
In a PERT network, the critical path represents the sequence of dependent tasks that takes the longest time to complete. Any delay in an activity on this path will directly result in a delay of the entire project's completion date. Identifying the critical path is essential for project managers to focus their resources and attention on the most time-sensitive tasks, ensuring that the project remains on schedule and that potential bottlenecks are managed effectively.

**62.** (A) The organization must put into place basic project management practices such as estimating software size and resources.
At the Repeatable Level (Level 2) of the Capability Maturity Model, an organization establishes basic project management practices to track cost, schedule, and functionality. These practices include estimating software size and resource requirements based on historical data. While processes are defined at the project level, the organization still relies heavily on individual expertise, and procedures may be abandoned during times of stress. This level provides a foundation for more advanced process standardization in subsequent stages.

**63.** (A) Gantt Chart
A Gantt chart is a project management tool that uses horizontal bars to plot activities against a specific time frame. The length of each bar represents the duration of a task, with the left end indicating the start and the right end showing the finish. This visual representation allows managers to easily monitor progress and see which tasks are currently underway. While useful for scheduling, Gantt charts do not typically show complex interdependence or precedence relationships.

**64.** (C) Because applying multiple CMM models that were not integrated within an organization was costly in training and appraisals.
The CMMI project was formed because organizations found it difficult and costly to apply multiple, non-integrated Capability Maturity Models simultaneously. Different models for software, systems engineering, and product development required separate training and appraisals, leading to inefficiency and confusion. CMMI provides a unified framework that integrates these disciplines, allowing organizations to streamline their process improvement efforts, reduce costs, and improve overall performance across various functional areas through a single, cohesive maturity model.

**65.** (A) Reverting to an ad hoc process model during times of stress.
Successful project management requires maintaining disciplined and organized processes, even during challenging situations. Reverting to ad hoc or chaotic methods when under stress is a characteristic of lower maturity levels and often leads to project failure. Instead, managers should focus on leveraging team abilities, assigning meaningful work, and providing opportunities for career development. Consistent adherence to established procedures ensures stability and predictability, which are critical for delivering complex software systems on time and within budget.

**66.** (A) Allowing each local unit to customize databases due to diverse usage and definitions.
A centralized data environment is designed to consolidate and integrate data into a single cohesive unit, ensuring consistency across the organization. Allowing each local unit to customize databases with diverse definitions would lead to data redundancy and inaccuracies, which contradicts the primary goals of centralization. Instead, a central approach assures that all data reflects the same time value and provides management with a clear, unified view of the organization's information flow and operational performance.

**67.** (C) Ensuring that all decisions are made strictly by a single top executive.
A Group Decision Support System is specifically designed to facilitate collaborative decision-

Click Here to Buy book on Amazon

perspective of the business, rather than relying on fragmented data from isolated departments that might use inconsistent definitions or time values.

**82.** (A) A terminal achievement that has no duration and simply tells that an activity has ended or begun.
In a PERT chart, an event is a terminal achievement that represents the beginning or end of an activity. Unlike activities, which have a specific duration and consume resources, events are points in time and have zero duration. They serve as milestones to track progress and indicate that necessary preceding tasks have been completed. By focusing on events, project managers can clearly define the sequence of work and ensure that the project is moving toward its final objectives.

**83.** (D) Improving job satisfaction by getting them interested in their jobs and recognizing their efforts spontaneously.
To maintain a satisfied and effective project staff, a manager should focus on improving job satisfaction by getting team members interested in their work. Recognizing their efforts spontaneously and providing opportunities for advancement and ability usage helps build a strong, motivated team. Relying solely on repetitive tasks or automated tools for performance evaluation can lead to boredom and turnover. Instead, personal engagement and professional development opportunities are key to retaining talent and ensuring long-term project success and stability.

**84.** (C) By defining a scale for measuring process maturity, allowing accurate comparison of process capability and serving as a blueprint for improvement.
The Capability Maturity Model assists organizations worldwide by providing a standardized scale for measuring process maturity. This allows companies to accurately compare their process capabilities with others and serves as a blueprint for continuous improvement. By defining the specific steps needed to move from a chaotic, ad hoc environment to a disciplined and optimized process, the CMM helps organizations enhance their software development quality, reliability, and efficiency, which is essential for competing in a global market.

**85.** (C) It describes the implementation activities of the key process area.
The "Activities Performed" common feature in the Capability Maturity Model describes the specific implementation activities required to achieve the goals of a Key Process Area. It outlines the work that must be done, such as conducting peer reviews or tracking project schedules. This feature is essential for institutionalizing processes within an organization, ensuring that the practices become a regular part of the development culture and are consistently followed across different projects to maintain high standards of quality.

**86.** (B) Horizontal bars - Show precedence relationship among the tasks
While horizontal bars in a Gantt chart are effective for showing the duration and schedule of individual tasks, they do not typically represent complex precedence relationships among tasks. These bars indicate when an activity starts and finishes relative to a time frame. To visualize the intricate dependencies and interconnections between tasks, project managers usually rely on PERT charts. Gantt charts are best suited for simple scheduling and monitoring progress against a timeline rather than mapping interdependent workflows.

**87.** (A) Only I
A modern data center must incorporate sufficient redundancy to guarantee round-the-clock connectivity and connect to multiple communication networks to avoid disruptions. In contrast, a Single Point of Failure is highly undesirable, as it creates a vulnerability that can stop the entire system from working. High-availability facilities are designed to eliminate SPOFs by duplicating critical components like power supplies and cooling systems, ensuring that business operations can continue even if an individual part fails or requires maintenance.

**88.** (B) Avoiding technical problems and delegating design details entirely to programmers.
A successful project manager must be able to handle technical problems and remain engaged with the design details of the system. While they delegate tasks, they must understand the

NODIA

on the logical sequence and timing of events to determine the project schedule. While PERT is excellent for managing time and workflow, it typically does not display the precise financial costs associated with each individual activity, which are usually tracked through other project management tools.

**75.** (D) Redundancy should be eliminated to isolate all SPOFs in a data centre.
A Single Point of Failure is any part of a system that, if it fails, will stop the entire system from working. SPOFs are highly undesirable in data centers aiming for high availability. To guarantee 24 x 7 operation, organizations must implement redundancy to ensure that no single component's failure can disrupt service. Therefore, management should focus on eliminating SPOFs by adding redundant systems and infrastructure, rather than eliminating redundancy to isolate these critical failure points.

**76.** (D) It completely eliminates the need for contingency planning once the network is drawn.
Project management involves planning, designing, and implementing systems to meet specific goals, managed by a project leader who schedules tasks and evaluates progress. It requires estimating resource requirements and producing quality systems on time. Crucially, project management does not eliminate the need for contingency planning. Even with a well-drawn network and schedule, managers must remain prepared for unexpected challenges and changes by developing backup plans to ensure the project continues toward its successful completion.

**77.** (D) P-2, Q-4, R-1, S-3
The CMM levels represent an evolutionary path for process improvement. Level 1 is characterized by ad hoc, chaotic processes. Level 2 establishes basic project management but remains dependent on individuals during stress. At Level 3, standards are codified and peer reviews are introduced. Finally, Level 5 focuses on continuous improvement by evaluating new processes and technologies. This framework allows organizations to assess their current capabilities and develop a clear blueprint for achieving higher levels of maturity.

**78.** (A) II, IV, I, III
To draw a Gantt chart, a manager first identifies the activities and tasks within a project stage. Next, they determine the specific tasks for each activity and estimate their completion times. The third step involves determining the total estimated time for each activity and obtaining an agreement to proceed. Finally, the activities are plotted on the chart, and progress is reviewed and recorded periodically to ensure the project remains on schedule and within its defined timeframe.

**79.** (B) Level 3: Defined Level
An organization achieves the Defined Level (Level 3) of the CMM when it has codified its software development practices into a standard set of procedures. At this level, training is provided, and peer reviews are conducted to maintain quality. Importantly, these processes belong to the organization and are not abandoned during times of stress. This standardization ensures that projects are managed consistently across the firm, providing a stable foundation for quantitative measurement and continuous process improvement.

**80.** (C) I, II, and III
Each maturity level in the CMM, except the Initial Level, is composed of several Key Process Areas that define a cluster of related activities. These KPAs are organized into five sections called Common Features, which specify the key practices required to achieve the KPA's goals. The framework describes an evolutionary improvement path consisting of five maturity levels, not ten. By focusing on these structured components, organizations can systematically improve their software processes and achieve higher performance.

**81.** (C) The clearer framework provided by data interaction and flow for understanding how various functions interact and affect the unit.
Management awareness in a centralized data environment refers to the clearer framework provided by integrated data interaction and flow. When all information is consolidated into a single pool, managers can better understand how different functions interact and affect the entire organization. This holistic view enables leaders to make more informed decisions based on a unified

Downloaded from www.pdf.tube

with rigid central control; rather, they delegate authority to local users. This autonomy is what makes maintaining a unified and synergistic global informational model so challenging for an organization's management.

**109.** (D) Due to Building risks involving threats posed by other applications and multi-tenant neighbours.
Locating a data center under a kitchen or in a basement is discouraged due to significant building risks. Kitchens pose threats from water leaks and fire hazards, while basements are prone to flooding. These locations expose critical infrastructure to dangers created by other applications and multi-tenant neighbors within the same facility. To ensure high availability, data centers should be placed in areas that minimize these environmental threats, providing a more stable and secure environment for the hardware and data storage systems.

**110.** (A) I and II
Data Mesh is a modern approach for analytical data management based on a distributed architecture. It distributes data ownership to domain-specific teams, who serve data as a product. Unlike traditional models, it does not require users to transport data to a central lake or warehouse before accessing it. By closing the gap between data generation and consumption, Data Mesh enables real-time decision-making and avoids the bottlenecks associated with centralized infrastructure teams, leading to more agile and responsive data management strategies.

**111.** (A) I, II, and III
A proper Disaster Recovery setup requires establishing a DR site in a different seismic zone to mitigate concentration risk. Connectivity should be maintained through redundant links like MPLS and wireless connections. Additionally, a Network Aggregation Point should connect both the DC and DR sites to ensure seamless service transition. Placing all backup servers in the same facility as the primary data center would be an ineffective setup, as a single event could destroy both the primary and backup systems simultaneously.

**112.** (B) P-2, Q-1, R-2, S-1
Data environments have distinct advantages and disadvantages. Data redundancy and difficulty in corporate-level reporting are common disadvantages of a decentralized data environment. Conversely, data integration and enhanced management awareness through a unified flow of information are significant advantages of a centralized data environment. By understanding these trade-offs, organizations can better decide whether to consolidate their information into a single pool or distribute it among semi-independent units to best support their operational needs and strategic management goals throughout the firm.

**113.** (C) Loss of Synergy
When the global informational model is fragmented in a decentralized environment, the organization often experiences a loss of synergy. This occurs because different units operate with inconsistent data definitions and models, making it difficult to coordinate activities and achieve firm-wide objectives. While decentralization offers local flexibility, the lack of a unified data framework can prevent the organization from realizing the full value of its information assets. This fragmentation necessitates stronger central coordination to ensure that disparate systems can still work together effectively.

NODIA

**114.** (B) A Tier III data center is concurrently maintainable, allowing for planned maintenance without disrupting operations.
A Tier III data center is characterized by being concurrently maintainable, which allows for planned maintenance of cooling and power systems without disrupting computer hardware operation. This provides a high level of availability, though it is not completely fault-tolerant like a Tier 4 facility. Tier 4 centers are designed to handle both planned and unplanned activities without outages, while Tier III centers can still be affected by spontaneous failures. Most banks strive for higher tier ratings to ensure 24 x 7 service delivery for their customers.

**115.** (D) P-3, Q-4, R-1, S-2
Data center risks fall into several categories. Geographic and regional risks include natural disasters like tornadoes and earthquakes. Site-related risks involve external factors such as

technical challenges faced by the team to provide effective guidance and make informed decisions. Other essential qualities include flexibility, adaptability, and strong communication skills. A manager who avoids technical issues risks losing credibility and may fail to anticipate bottlenecks or quality concerns that could delay the project.

**89.** (A) Optimizing Level
At the Optimizing Level (Level 5) of the CMM, the organization focuses on continuous process improvement. This involves using quantitative process measures to evaluate new candidate processes and determine the efficacy of introducing innovative technologies. By proactively identifying and addressing weaknesses, organizations at this level can enhance their productivity and software quality. This stage represents the highest level of maturity, where the entire firm is dedicated to refining its processes to achieve peak performance and adapt to changing industry trends.

**90.** (A) It describes a path from a mature and disciplined process to an ad hoc, immature process.
The Capability Maturity Model describes a path from an immature, ad hoc process to a mature and disciplined one, not the other way around. Introduced in 1987 by the Software Engineering Institute at Carnegie Mellon University, it was originally designed to evaluate the capability of government contractors to perform software projects. CMM provides a framework for organizations to systematically improve their development processes, moving through five distinct maturity levels to achieve higher quality, predictability, and efficiency in their operations.

**91.** (B) User Confidence
In a decentralized database environment, users often feel a greater sense of ownership over "their data," leading to increased user confidence. Because the data is managed locally, any flaws or inaccuracies can be readily traced back to the group responsible, encouraging people to take an active interest in its protection and accuracy. This local accountability fosters a culture of responsibility and pride, ensuring that the database remains a reliable and valuable asset for the specific organizational units it serves.

**92.** (C) The age of the building and compliance with electric safety codes.
Site-related risks for a data center typically include factors like heavy population causing power overloads, trees near utility lines, and soil types affecting grounding. While the age of the building and its compliance with safety codes are important considerations, they are generally categorized under Building Risks rather than Site-related Risks. Building risks focus on the specific structural and operational threats posed by the facility itself and its other occupants, such as the location of the data center within the building.

**93.** (C) Universal data dialects unification
Decentralized data environments are characterized by functional specialization, user proximity, and the ability to accommodate local differences in practices. However, they often struggle with data dialects, where different units use varying definitions for the same data. Therefore, the unification of universal data dialects is a goal of centralization rather than a concept associated with decentralization. In a decentralized setup, the lack of central control often leads to a dispersion of data models that can make corporate-level reporting more challenging.

**94.** (C) It is highly vulnerable to operational errors causing immediate system-wide outages.
A Tier 4 data center is the highest level of availability, designed to be completely fault-tolerant with no single points of failure in its power and cooling infrastructure. It is specifically engineered to allow for unplanned activities, including spontaneous hardware failures, without disrupting operations for users. Consequently, it is not highly vulnerable to operational errors causing immediate system-wide outages; instead, its robust redundancy and automated recovery mechanisms ensure continuous service, making it ideal for critical enterprise-scale applications and high-availability needs.

**95.** (B) Web 3.0 (Decentralized Web)
Web 3.0 represents a movement toward a decentralized web that returns to the original vision of a neutral network where everyone can participate without relying on single central organizations. It leverages technologies like block-chain to distribute control and data, enhancing

Click Here to Buy book on Amazon

data depending on the specific problem being addressed. This overlap necessitates flexible information systems that can provide various levels of detail and context to support the complex and interconnected nature of management roles within an organization.

**54.** (C) MIS cater to a much larger user group dealing with structured and simpler problems.
Providing user-specific presentation capabilities in a conventional Management Information System is very expensive because these systems cater to a much larger user group compared to an Executive Information System. MIS users typically handle structured and simpler problems, where standardized reports are more cost-effective. In contrast, an EIS is tailored for a small group of senior executives whose unique strategic needs justify the high cost of developing highly customized and multidimensional data visualization tools.

**55.** (A) I, II, III, and V
Decision Support Systems are designed to be adaptive over time, although changes may take several weeks or months to implement. They feature integrated subsystems that process data along broad functional lines and utilize comprehensive databases managed by a DBMS. While the output is directed to personnel at all levels, a key characteristic is that the system should be easy to use, not requiring extensive programming knowledge by the manager to perform complex analyses.

**56.** (A) Management Information System (MIS)
A Management Information System is designed to support decision-making and visualize information to help users identify problems within an organization. While it provides structured reports and summaries of operations, it does not necessarily include the advanced analytical models and interactive problem-solving facilities found in a Decision Support System. MIS serves as a critical link between transaction processing and higher-level management by organizing raw data into meaningful information for control and planning.

**57.** (A) P-4, Q-1, R-3, S-2
Collaborative computing encompasses various types of software and tools. E-mail and calendar programs are fundamental software associated with collaboration. Lotus Notes and Novell Groupwise are classic examples of groupware applications. Brainstorming tools provide alternative generation capabilities within a GDSS framework. Synchronous groupware components, such as video conferencing, enable real-time communication among team members, ensuring that groups can work together effectively regardless of their location or the timing of their contributions.

**58.** (A) Operational Information
When a branch manager compares daily transaction counts and deposit volumes against budgeted figures, they are using operational information. This type of data is detailed and focused on the short-term control of routine activities. It allows managers to monitor performance at the ground level and take corrective actions to ensure that daily operations align with established targets. Operational information is foundational for the smooth functioning and efficiency of an organization's primary business processes.

**59.** (C) To serve the information needs of managers at the highest organizational levels by combining internal and external data.
The primary purpose of an Executive Information System is to serve the specialized information needs of managers at the highest organizational levels. By combining internal operational summaries with external market data, an EIS provides a comprehensive view of the factors critical to achieving strategic objectives. These systems utilize advanced visualization tools to present multidimensional information, enabling senior leaders to identify trends, monitor organizational health, and make informed decisions that shape the future direction of the company.

**60.** (B) The rapidly decreasing costs of computer storage and improvements in DBMS.
The adoption of distributed decision support systems is primarily justified by the rapidly decreasing costs of computer storage and significant improvements in Database Management Systems. These economic factors make it feasible for organizations to deploy powerful analytical tools across multiple

NODIA

**102.** (A) The database has a narrower audience and tends to serve the individual user better than a centralized database.
User proximity in a decentralized database environment provides the advantage of serving a narrower audience, which often results in the system being more responsive to the individual user's specific needs. Because the data is managed locally, it can be tailored to the functional requirements of the department it serves, rather than conforming to a broad and potentially rigid corporate model. This localized focus enhances the utility of the database for its primary users, fostering a stronger sense of ownership and data integrity.

**103.** (B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
Adding redundant utility feeds and carrier lines is a critical strategy to reduce the likelihood of power and communication outages at a data center. While it is true that redundant lines should be mandatory for businesses relying on high availability, this statement serves more as a best practice recommendation rather than a direct logical explanation for how redundancy physically decreases failure likelihood. Both statements highlight the importance of infrastructure reliability, but the reason describes a policy rather than a technical cause-and-effect relationship.

**104.** (D) Block-chain is essentially a distributed database or ledger where every event is registered as an unalterable block.
Block-chain is essentially a distributed database or ledger where every transaction or event is registered as an unalterable block in a chronological chain. This technology eliminates the need for a centralized registry, as the ledger is maintained across a network of members. While it provides a secure and transparent way to record data, it does not completely replace existing banking systems like NEFT. Instead, block-chain offers a new framework for decentralized applications, digital currencies, and secure, tamper-proof record-keeping in various industries.

**105.** (C) P-4, Q-1, R-3, S-2
A robust disaster recovery setup includes several critical components. The primary Data Centre is where the organization's data primarily resides. A Disaster Recovery site should be established in a different seismic zone to ensure continuity if the primary facility fails. Redundancy is provided through diverse communication links like MPLS and 3G/4G connections. Finally, a Network Aggregation Point connects both the DC and DR, facilitating the seamless transition of services and data during a major disruption or system outage.

**106.** (C) I and III
In a decentralized environment, downloading involves extracting data from a central source and reformatting it for local use. Because these links are often indirect, rules regarding data modification and sharing must be carefully documented to prevent inconsistencies. Uploading also requires careful management to ensure data integrity. By establishing clear protocols for how data moves between central and local systems, organizations can maintain a reliable information flow while benefiting from the flexibility and responsiveness of a distributed data architecture across multiple units.

**107.** (A) I, II, III, and IV
A Tier III data center is concurrently maintainable, meaning it allows for planned maintenance of power and cooling systems without disrupting hardware operations. It typically offers N+1 redundancy, providing a higher level of availability than lower tiers. However, while it handles planned events well, unplanned activities such as spontaneous failures can still cause an outage. Unlike Tier IV, it is not completely fault-tolerant, making it suitable for organizations that need high availability but can tolerate occasional, unforeseen downtime for repairs.

NODIA

**108.** (C) Assertion (A) is true, but Reason (R) is false.
Coordinating decentralized databases is a difficult task because they are often managed by semi-independent units that may use varying data definitions and models. This dispersion of control can lead to data redundancy and inconsistencies. The reason provided is false because, by definition, decentralized databases are not strictly property of corporate management

user privacy and autonomy. This trend contrasts with the current centralized model dominated by a few large entities. By enabling peer-to-peer interactions and decentralized governance, Web 3.0 aims to create a more resilient, open, and equitable digital ecosystem for all users.

**96.** (B) Disconnecting the city Network Aggregation Point from the DR
Redundancy measures for communication between branches and data centers include using MPLS links, 3G/4G connections, and alternate lease lines from different telecom operators. These backups ensure that services continue even if a primary provider fails. Disconnecting the city Network Aggregation Point from the Disaster Recovery site would actually eliminate a critical connection and create a single point of failure, which is the opposite of providing redundancy. Proper DRS setups require multiple, diverse links to maintain high availability and business continuity during disruptions.

**97.** (C) Both I and II
A decentralized data environment consists of multiple databases serving different organizational segments, allowing local units to operate semi-independently. Linkages between these systems may involve sharing common data or downloading reference data from a central source. While this approach provides flexibility and user proximity, it also requires carefully documented rules for data modification and sharing to ensure consistency and prevent errors. This structure allows organizations to balance the benefits of local control with the need for coordinated, firm-wide information management.

**98.** (A) It provides a connectivity layer that requires costly data transfers and residency concerns.
Data Mesh is a modern, distributed architecture that views data as a product and delegates ownership to domain-specific teams. This approach aims to steer enterprises toward real-time decision-making by closing the gap between data generation and analysis. A key advantage is that it provides a connectivity layer that actually avoids costly data transfers and residency concerns, rather than requiring them. By allowing users to access data where it resides, Data Mesh improves efficiency and enables more agile, domain-driven data management.

**99.** (B) Only II
When selecting a facility for a data center, management must evaluate whether the site meets the organization's operating requirements for the first five years to accommodate short-term and long-term size needs. While factors like earthquakes and grounding systems are critical for risk assessment, the primary concern for size requirements is ensuring the facility can handle anticipated growth and equipment needs. This projection ensures that the organization does not quickly outgrow the space, avoiding the high costs associated with early relocation.

**100.** (C) Dispersion of data and local definitions make aggregate, cross-unit reports more difficult to prepare.
Corporate-level reporting is challenging in a decentralized data environment because information is dispersed across multiple semi-independent units. Furthermore, local units often develop their own data dialects or definitions that differ from the central standard. This lack of uniformity makes it difficult to prepare aggregate, cross-unit reports, as the data must be carefully reformatted and reconciled to ensure accuracy. This dispersion of data and ownership can hinder top management's ability to get a unified view of the entire organization's performance.

**101.** (A) P-3, Q-1, R-4, S-2
Various information system concepts have distinct characteristics. The CMM describes an evolutionary improvement path for processes. A PERT chart emphasizes determining the critical path and precedence relationships without looping. Groupware enables both synchronous and asynchronous collaboration and information sharing. A decentralized database is characterized by user proximity and the potential for data redundancy. Understanding these features helps organizations choose the right tools and strategies to support their specific management, development, and operational needs in a digital environment.

Downloaded from www.pdf.tube

power overloads from heavy populations or trees interfering with utility lines. Building risks focus on internal issues like sags caused by heavy loads or the facility's location. Economic risks encompass financial factors such as tax incentives, utility rates, and land costs. Evaluating these risks comprehensively helps management select the most secure and cost-effective site for their critical operations.

**116.** (D) Data is fed downwards from senior parent management to conform to strict central standards.
In a decentralized database environment, local units often have distinct data requirements and accounting practices, which can make decentralization a better choice. Because each unit is essentially a separate organization with specific needs, opportunities for compromise are often limited. The statement that data is fed downwards from senior management to conform to strict central standards is incorrect, as decentralization emphasizes local autonomy and proximity to the user, allowing individual units to manage their data in ways that best support their unique functional activities and objectives.

**117.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Financial institutions are moving toward Tier-IV data centers because the criticality of their services has increased with the extension of 24 x 7 banking operations. A Tier-IV facility provides the highest level of availability and fault tolerance, ensuring that even unplanned failures do not cause outages. This level of reliability is essential for maintaining customer trust and meeting the high uptime requirements of modern digital banking services, where any disruption can have significant financial and reputational consequences for the organization.

**118.** (D) Data Redundancy
Data redundancy occurs when the same piece of data is held in two or more separate places within an organization. This condition often leads to discrepancies and inaccuracies, as updates may not be applied consistently across all locations. In a decentralized environment, redundancy is a common challenge that requires increased management control to ensure data integrity. While it can improve local access speed, the risks of having conflicting information often outweigh these benefits, necessitating strategies like data integration to maintain a single version of truth.

**119.** (A) I, II, and III
Economic risks associated with data center site selection include factors that directly impact the facility's financial viability and operating costs. These include tax and other incentives provided by the state, the overall operating expenses relative to alternative sites, and the availability of skilled labor in the region. While urban or rural area types can influence power consumption, they are more typically categorized under Site-related Risks. Focusing on economic factors helps management ensure the long-term affordability and sustainability of the chosen location for their critical infrastructure.

**120.** (C) Both I and II
Block-chain technology offers significant benefits for banking, particularly in trade finance, by mitigating fraud risks like the multiple discounting of the same invoice. By creating an unalterable record of transactions, it provides a transparent and secure way to track assets. Additionally, block-chain allows all events related to a loan to be placed on the "block," enabling all members to access consistent information and make more informed decisions. This distributed ledger approach enhances trust and efficiency in complex financial processes involving multiple stakeholders and high-value transactions.

**121.** (D) Sags within the building and for surrounding miles
When a data center is located in a multi-tenant building with heavy industrial machinery, the large power draws from that equipment can cause significant sags in the building's electrical supply. These voltage drops can extend for several miles and disrupt the sensitive hardware required for data processing and storage. This is a specific example of a building risk, where the activities of other tenants directly threaten the stability and availability of the organization's information systems, necessitating specialized power conditioning or the selection of a more isolated facility.

NODIA

May/June 2021

**8.** Match the abstraction level in List I with its characteristics in List II and choose the correct option.

List I: (Abstraction level)

P. Physical level
Q. Logical level
R. View level
S. Data abstraction

List II: (Characteristics)

1. Highest level describing only part of the database.
2. Decides what information is kept and the relationships among data.
3. Describes how data are actually stored.
4. Hides certain details of how data are stored and maintained.

(A) P-1, Q-2, R-3, S-4
(B) P-3, Q-2, R-1, S-4
(C) P-2, Q-3, R-4, S-1
(D) P-4, Q-1, R-2, S-3

Oct/Nov 2009

**9.** Identify the incorrect statement regarding the Generic data model.

(A) They are generalizations of conventional data models.
(B) They define standardized general relation types.
(C) They are developed as an approach to solve shortcomings of conventional data models.
(D) They complicate data exchange and data integration by avoiding standardization.

May/June 2018

**10.** Read the following statements regarding file processing systems:

I Data isolation occurs because data is scattered in various files at different locations and in different formats.
II Integrity problems are easily resolved by writing new application programs that retrieve appropriate data formats.

Which of the statements is/are correct?

(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

Oct/Nov 2025

**11.** Match the DBA function in List I with its description in List II and choose the correct option.

List I: (DBA function)

P. Scheme definition
Q. Granting of authorization
R. Integrity constraints specification
S. Storage structure and access method

List II: (Description)

1. Create appropriate access methods.
2. Grant access to users as decided by the data owner.
3. Maintain data consistency.
4. Create database definitions stored permanently in the data dictionary.

(A) P-4, Q-2, R-3, S-1
(B) P-1, Q-3, R-2, S-4
(C) P-2, Q-4, R-1, S-3
(D) P-3, Q-1, R-4, S-2

May/June 2012

**12.** Identify the incorrect statement regarding the disadvantages of using file processing systems.

(A) Data redundancy leads to inconsistent states when data is modified in only one location.
(B) It is difficult to change programs to enforce new consistency constraints.
(C) Environments allow needed data to be retrieved in a convenient and efficient manner.
(D) Allowing multiple users to concurrently access and update data is very difficult to supervise.

Oct/Nov 2014

**13.** Which of the following is considered the very first data model where all data used are kept in the same plane?

(A) Flat data-model
(B) Semantic data model
(C) Entity-Relationship model
(D) Relational model

May/June 2019

**14.** Which level of data abstraction describes how the data are actually stored and details complex low-level data structures?

(A) Logical level
(B) View level
(C) Physical level
(D) Generic level

Click Here to Buy book on Amazon

# CHAPTER 06

# Database Management Systems

NODIA

Oct/Nov 2023

**1.** The following question consists of two statements — Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): In a conventional file processing system, ensuring that a money exchange transaction is executed completely or not at all is very difficult.
Reason (R): File processing systems inherently struggle to enforce the atomicity property during system failures.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2008

**2.** In the Entity-Relationship (ER) model, what represents the logical association among entities?
(A) Attribute
(B) Domain
(C) Relationship
(D) Cardinality

Oct/Nov 2016

**3.** In the context of database management, how does data redundancy primarily affect a file processing system?
(A) Decreased storage usage through localized data retention.
(B) Difficulty in isolating appropriate specific data formats.
(C) Higher costs and potential data inconsistency.
(D) Lowered costs associated with direct data access methods.

May/June 2024

**4.** A school database maintains records of its students. Under the ER Model design, "Student" represents a real-world entity. Which of the following best represents the properties of this entity?
(A) One to many
(B) First-order predicate logic
(C) Name, age, class
(D) Flat data mapping

Oct/Nov 2007

**5.** Identify the correct pair regarding levels of data abstraction.
(A) Physical level - Describes what data are stored and relationships among those data.
(B) View level - Describes only a part of the entire database for a specific user.
(C) Logical level - The lowest level of abstraction describing complex data structures.
(D) Conceptual level - Deals with the hardware storage devices directly.

May/June 2015

**6.** Which function of a Database Administrator (DBA) involves creating appropriate storage structures and access methods?
(A) Scheme definition
(B) Storage structure and access method
(C) Granting of authorization for data access
(D) Integrity constraints specification

Oct/Nov 2011

**7.** What defines a database management system (DBMS)?
(A) A collection of unrelated data organized for manual retrieval.
(B) A system for managing interrelated data and programs.
(C) A hardware architecture designed for physical data processing.
(D) A standalone program used for isolated data manipulation.

(D) Attributes with null values for missing data.

May/June 2014

**38.** An HR manager needs to find the employee numbers and names of all employees who joined after 1st Dec 2009. Which SQL query should they execute?
(A) select * from emp where empjoin < '01-DEC-09'
(B) select empname from emp where empjoin > '01-DEC-09'
(C) select empno from emp where empjoin = '01-DEC-09'
(D) select empno, empname from emp where empjoin > '01-DEC-09'

Oct/Nov 2013

**39.** Which type of database architecture generally guarantees a more limited form of ACID compliance called "eventual consistency"?
(A) Relational databases
(B) RDBMS architectures
(C) Normalized SQL databases
(D) NoSQL databases

May/June 2021

**40.** What defines a procedural query language?
(A) The user describes the information without giving a specific procedure for obtaining it.
(B) The database automatically determines the sequence of queries based on historical data.
(C) The language is used exclusively for hardware configuration.
(D) The user instructs the system to perform a sequence of operations.

Oct/Nov 2021

**41.** Match the ACID property in List I with its operational definition in List II and choose the correct option.
List I: (ACID property)
P. Atomicity
Q. Consistency
R. Isolation
S. Durability
List II: (Operational definition)
1. Transactions must be recorded in non-volatile memory to survive crashes.
2. Concurrent execution results in a state as if executed sequentially.
3. Transaction must be "all or nothing".
4. Transaction brings the database from one valid state to another based on defined rules.
(A) P-3, Q-4, R-2, S-1
(B) P-4, Q-3, R-1, S-2
(C) P-2, Q-1, R-4, S-3
(D) P-1, Q-2, R-3, S-4

May/June 2023

**42.** Read the following statements regarding database keys:
I A super key can contain extra attributes.
II A candidate key is a proper subset of a super key which identifies the entity uniquely.
III The primary key selected by the database designer cannot have null values.
Which of the statements are correct?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) (I), (II), and (III)

Oct/Nov 2018

**43.** Read the following statements regarding Views in a database:
I A view is a query that retrieves limited data derived from one or more tables.
II The tables from which the view is derived are known as base tables.
III Base tables can only be physical tables and never other views.
IV Most of the times, views are read-only.
Which of the given statements are correct?
(A) Only (I), (II), and (III)
(B) Only (I), (II), and (IV)
(C) Only (II), (III), and (IV)
(D) All of the above

May/June 2016

**44.** Which SQL clause consists of the condition involving attributes of the tables that appear in the from clause?
(A) select
(B) from
(C) insert
(D) where

Oct/Nov 2022

**45.** The following question consists of two statements — Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): The Durability property ensures

Downloaded from www.pdf.tube

**Oct/Nov 2006**

**15.** Match the Mapping Cardinality in List I with its conceptual meaning in List II and choose the correct option.

List I: (Mapping Cardinality)

P. one to one
Q. one to many
R. many to one
S. many to many

List II: (Conceptual meaning)

1. Multiple entities associated with multiple entities.
2. Single entity associated with multiple entities.
3. Single entity associated with a single entity.
4. Multiple entities associated with a single entity.

(A) P-3, Q-2, R-4, S-1
(B) P-2, Q-3, R-1, S-4
(C) P-1, Q-4, R-3, S-2
(D) P-4, Q-1, R-2, S-3

**May/June 2020**

**16.** Which underlying file system does Hadoop utilize to act as the bedrock of Big Data today?
(A) Hadoop Distributed File System (HDFS)
(B) New Technology File System (NTFS)
(C) Extended File Allocation Table (exFAT)
(D) Relational File Structure System (RFSS)

**Oct/Nov 2010**

**17.** The following question consists of two statements — Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.

Assertion (A): In a Semantic Data Model (SDM), the entity type "person" is treated as a whole entity rather than being broken down into parts like spouse, children, and job.

Reason (R): Relational models inherently handle conceptual definitions of data better than SDM by merging all relationships into a single table.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2005**

**18.** A large enterprise stores immense volumes of unstructured and structured data across thousands of server nodes. To manage this without the limitations of conventional file processing, the enterprise adopts Hadoop. Which foundational technology within Hadoop directly negates the traditional issues of scattered, isolated files?
(A) Hadoop File System (HDFS)
(B) Embedded DML
(C) Semantic Data Model (SDM)
(D) Structured Query Language (SQL)

**Oct/Nov 2022**

**19.** Which of the following is a correct statement regarding the Relational Model?
(A) Storing all data on a single plane without atoms.
(B) Requiring multiple rows to contain unique values.
(C) Restricting columns from using the same domains.
(D) Defining a table as an n-ary relation via logic.

**May/June 2016**

**20.** A database administrator for a banking institution decides to store customer transaction histories alongside account details and establishes a direct relationship between them. The administrator does not concern themselves with the byte-level storage mechanism on the hard drives. Which level of data abstraction is the administrator actively working at?
(A) Logical level
(B) Physical level
(C) View level
(D) Semantic level

NODIA

**Oct/Nov 2018**

**21.** Identify the incorrect statement regarding the functions of a Database Administrator (DBA).
(A) Scheme definition - Creating database definitions stored permanently in the data dictionary.
(B) Storage structure and access method - Creating appropriate storage structures.
(C) Granting of authorization - Maintaining data consistency across atomic values.
(D) Integrity constraints specification - Maintaining data consistency.

Oct/Nov 2016

**53.** Identify the incorrect statement regarding Structured Query Language (SQL).
(A) Commands used to insert or extract table data.
(B) A subset of SQL used to modify database objects.
(C) Users specifying a manual sequence of operations.
(D) SQL used within languages like C and COBOL.

May/June 2019

**54.** Read the following statements regarding database architectures:
I Relational databases require a rigid schema that is difficult for DBAs to modify on the fly.
II Relational software uses primary and foreign keys to establish relationships.
III Normalization eliminates the need to redundantly store related data in multiple tables.
IV File-based Hadoop clusters are utilized in big data environments.
V NoSQL software was partly created due to the rigid schema limitations of relational technology.
Which combination represents the correct statements?
(A) Only (I), (II), (III), and (V)
(B) Only (II), (III), (IV), and (V)
(C) Only (I), (III), and (IV)
(D) All of the above

Oct/Nov 2006

**55.** Match the SQL term in List I with its function in List II and choose the correct option.
List I: (SQL term)
P. DDL
Q. DML
R. select clause
S. from clause
List II: (Function)
1. Lists the tables to be scanned in the evaluation.
2. Lists the attributes desired in the result of the query.
3. Commands to insert data into tables and extract data.
4. Commands to add, modify or delete tables.
(A) P-4, Q-3, R-2, S-1
(B) P-3, Q-4, R-1, S-2
(C) P-2, Q-1, R-4, S-3
(D) P-1, Q-2, R-3, S-4

May/June 2020

**56.** Read the following statements regarding the structure of relational databases:
I For each attribute in a table, the set of permitted values is called the domain of that attribute.
II Null values in an attribute indicate that the value is known and rigidly defined.
Which of the statements is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

Oct/Nov 2010

**57.** Which of the following is NOT a property of an ACID-compliant database system?
(A) Eventual consistency
(B) Atomicity
(C) Isolation
(D) Durability

May/June 2005

**58.** Which component of SQL includes commands used to add, modify, or delete tables in a database?
(A) Data Definition Language (DDL)
(B) Data Manipulation Language (DML)
(C) Embedded DML
(D) Information Retrieval Query Language

Oct/Nov 2025

**59.** Read the following statements regarding RDBMS versus other DBMS types:
I RDBMS supports referential integrity and adherence to ACID properties.
II Many NoSQL databases guarantee strict ACID compliance in all scenarios instead of eventual consistency.
Which of the statements is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

May/June 2018

**60.** Which statement correctly describes the function of the select clause in SQL?
(A) It lists the relations that are to be scanned in

Click Here to Buy book on Amazon

(C) Saving multi-valued data in normalized relations.
(D) Each column containing values from the same domain.

**May/June 2011**

**30.** Read the following statements regarding the levels of data abstraction:
I The logical level of abstraction is used by database administrators who decide what information is to be kept.
II At the physical level, complex low-level data structures are described in detail.
III The view level ensures all users must access and view the entirety of the database concurrently.
Which of the statements is/are correct?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) (I), (II), and (III)

**Oct/Nov 2020**

**31.** In an "Employee" table containing attributes Employee Number, Name, Address, and Join Date, the database designer selects Employee Number to uniquely identify each row. Employee Number will not be repeated for two different employees. In this context, what is Employee Number?
(A) Foreign Key
(B) View Level Attribute
(C) Primary Key
(D) Null Key

**May/June 2017**

**32.** The following question consists of two statements — Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): Using a view, an administrator can restrict user access to specific parts of a table while allowing simple queries to retrieve results from complicated underlying structures.
Reason (R): Views physically duplicate the data into a new standalone table, isolating it from the base tables.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2019**

**33.** Which statement correctly distinguishes Relational databases from flat-file databases?
(A) Relational databases are self-contained in a single table, unlike flat-file databases.
(B) A single relational database can be spread across several tables.
(C) Relational databases require all attributes to contain null values.
(D) Flat-file databases utilize primary and foreign keys to establish relationships.

**May/June 2025**

**34.** Identify the incorrect statement regarding the Consistency property of ACID.
(A) Ensures transitions between valid states only.
(B) Ensures data is written based on defined rules.
(C) Includes constraints, cascades, and triggers.
(D) Guarantees total correctness of applications.

**Oct/Nov 2005**

**35.** Which of the following is NOT a basic clause in the structure of the SQL language?
(A) isolate
(B) select
(C) from
(D) where

**May/June 2006**

**36.** A bank processes a bulk transfer of funds. The SQL statements execute successfully, and the database commits the transaction. One second later, the entire data center loses power. When systems are restored, the transaction is fully intact. Which property guarantees this behavior?
(A) Durability
(B) Isolation
(C) Atomicity
(D) Consistency

**Oct/Nov 2024**

**37.** What defines a super key in a relational database?
(A) Attributes that collectively identify an entity.
(B) Attributes identifying rows via foreign keys.
(C) Attributes representing relationships among tables.

Downloaded from www.pdf.tube

**122.** (C) Evaluating compatibility, functionality, speed, and technical support
When acquiring software, management evaluates key factors such as compatibility with current systems, functionality, processing speed, and the availability of technical support. This process ensures that the new application will work effectively within the organization's existing environment and meet the performance requirements of its users. Unlike custom development, acquisition relies on assessing pre-built solutions to find the best fit for organizational needs. This evaluation is critical for minimizing integration risks and ensuring that the chosen product provides a robust and reliable platform for business operations.

**123.** (C) The city Network Aggregation Point (NAP) is connected to both DC & DR with alternate lease lines from another telecom operator acting as a backup.
To ensure high availability and prevent service loss, organizations often connect their city Network Aggregation Point to both the primary Data Centre and the Disaster Recovery site. By utilizing alternate lease lines from a different telecommunication operator as a backup, the bank creates a redundant network topology. This setup ensures that if the primary provider fails, communication can be maintained through the secondary link. Such redundancy is essential for modern banking operations that rely on constant connectivity between branches and central processing facilities to serve their customers.

**124.** (A) The tax incentives offered by the state
Factors like weather, animals on lines, the use of underground wiring, and ground impedance are all critical considerations for assessing site-related risks to a data center's electrical and grounding systems. These physical factors directly impact the stability and safety of the facility's power infrastructure. In contrast, tax incentives offered by the state are categorized as economic risks. While important for the overall financial decision, they do not affect the technical reliability of the grounding or wiring systems necessary to protect the hardware and ensure continuous operation.

**125.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Establishing a Disaster Recovery site in a different seismic zone is a key strategy for mitigating concentration risk. By placing the DR site in a geographically distinct location, organizations ensure that a single natural disaster cannot disable both the primary and backup facilities. This setup allows the DR site to take over operations if the primary Data Centre fails, ensuring business continuity. This geographic separation is vital for maintaining the availability of critical financial services and protecting the organization's data assets from regional threats or large-scale emergencies.

NODIA
www.nodia.in

that once a transaction has been committed, it will remain so, even in the event of power loss.
Reason (R): To defend against power loss, transactions must be recorded in a volatile memory system.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2015**

**46.** Which of the following is NOT an attribute of keys in a relational database?
(A) A super key can contain extra attributes.
(B) A Primary Key is permitted to have multiple null values.
(C) The proper subset of a super key which identifies the entity uniquely is called a candidate key.
(D) The key selected by the database designer is called the Primary Key.

**Oct/Nov 2009**

**47.** The acronym ACID in database management stands for which of the following sets of properties?
(A) Atomicity, Consistency, Isolation, Durability.
(B) Atomicity, Centralization, Independence, Data.
(C) Authorization, Concurrency, Isolation, Power.
(D) Application, Consistency, Integrity, Speed.

**May/June 2010**

**48.** A relational database has an "Employee" table with a "Department Number" attribute. This "Department Number" attribute is the primary key of another table called "Department". What is the role of the "Department Number" attribute in the "Employee" table?
(A) Super Key
(B) Foreign Key
(C) Primary Key
(D) Candidate Key

**Oct/Nov 2007**

**49.** Normalization is a concept that applies strictly to which type of databases?
(A) Relational databases
(B) Flat-file databases
(C) Generic databases
(D) Semantic databases

**May/June 2024**

**50.** A user executes the SQL query: "select empcity from emp". What will be the output of this query?
(A) Displays all attributes and rows in the table.
(B) Inserts a new city into the existing table.
(C) Displays the empcity attribute for all records.
(D) Deletes all cities from the table structure.

**Oct/Nov 2014**

**51.** Two separate database users attempt to book the last available ticket for a flight at the exact same millisecond. The database system ensures that the transactions are processed such that the system state would be the same as if they were executed sequentially. Which property is being enforced?
(A) Processing concurrent tasks as if sequential.
(B) Executing all transaction commands as a unit.
(C) Recording data in non-volatile memory systems.
(D) Hiding storage details to simplify interaction.

**May/June 2012**

**52.** The following question consists of two statements — Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): A database designer must ensure that the designated Primary Key for a table does not contain null values.
Reason (R): A Primary Key uniquely identifies all the rows of a table, and a null value would indicate an unknown or non-existent identifier, violating uniqueness.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Click Here to Buy book on Amazon

May/June 2007

**22.** Which of the following is NOT listed as a disadvantage of using file processing systems?
(A) Data isolation
(B) Automatic data indexation
(C) Concurrency problems
(D) Integrity problem

Oct/Nov 2008

**23.** What is the definition of data abstraction in a database system?
(A) Relocating database servers to cloud environments.
(B) Storing data redundantly across multiple formats.
(C) Bypassing security controls with new applications.
(D) Hiding storage details to simplify interaction.

May/June 2022

**24.** Read the following statements about the Semantic Data Model (SDM):
I SDM defines the meaning of data within the context of its interrelationships with other data.
II SDM is an abstraction which defines how stored symbols relate to the real world.
III In SDM, an entity is very similar to a domain.
IV SDM breaks down an entity into parts across multiple tables to maximize physical data separation.
Which of the given statements are correct?
(A) Only (I), (II), and (III)
(B) Only (II), (III), and (IV)
(C) Only (I), (III), and (IV)
(D) All of the above

Oct/Nov 2015

**25.** What do data models fundamentally define in a Database Management System?
(A) The physical hardware configurations required for database servers.
(B) How the logical structure of a database is modelled and how data is connected.
(C) The specific programming languages used for querying the system.
(D) The graphical user interfaces presented to the end-users.

May/June 2013

**26.** Which statement correctly describes the requirement of "Atomicity" in database systems?
(A) Transactions partially applied when failures occur.
(B) Data separated across several physical locations.
(C) Multiple users updating the same data simultaneously.
(D) Transactions applied completely or not at all.

NODIA

Oct/Nov 2017

**27.** In an SDM framework, a database domain called "Person names" contains the values Bob, Sue, Jim, Betty, and Clyde. What do each of these names point to within the SDM structure?
(A) An object instance providing specific details.
(B) A standardized general relation type structure.
(C) A physical memory address on the hard drive.
(D) A flat data-model containing redundant fields.

May/June 2009

**28.** Match the disadvantage of file processing systems in List I with its description in List II and choose the correct option.
List I: (Disadvantage)
P. Data redundancy
Q. Integrity problem
R. Concurrency problem
S. Security problem
List II: (Description)
1. Multiple users accessing and updating data simultaneously without supervision.
2. Difficulty in applying constraints that involve several data items from different files.
3. Same data stored at various locations leading to higher storage cost.
4. Inability to restrict access to sensitive data for specific users.
(A) P-3, Q-2, R-1, S-4
(B) P-2, Q-3, R-4, S-1
(C) P-1, Q-4, R-2, S-3
(D) P-4, Q-1, R-3, S-2

Oct/Nov 2012

**29.** Which of the following is NOT a main highlight of the Relational Model?
(A) Storing data in tables specifically called relations.
(B) Each row in a relation containing a unique value.

the evaluation of the expression.
(B) It is used to list the attributes desired in the result of the query.
(C) It deletes tables in the database.
(D) It restricts access to a table based on user privileges.

**Oct/Nov 2023**

**61.** Match the Database Anomaly in List I with its characteristic in List II and choose the correct option.
List I: (Database Anomaly)
P. Update anomaly
Q. Insert anomaly
R. Delete anomaly
S. Data redundancy
List II: (Characteristic)
1. Removing data causes unintended loss of other unrelated data.
2. Storing the same data in multiple rows leading to higher storage.
3. Inability to add data because part of the record is missing and nulls are restricted.
4. Partial modification of replicated data leading to inconsistency.
(A) P-4, Q-3, R-1, S-2
(B) P-3, Q-4, R-2, S-1
(C) P-1, Q-2, R-3, S-4
(D) P-2, Q-1, R-4, S-3

**May/June 2008**

**62.** In the context of normalization, what is the definition of a non-prime attribute?
(A) An attribute that is not part of any candidate key.
(B) An attribute that is a part of one of the candidate keys.
(C) An attribute that contains multiple atomic values.
(D) An attribute that functions exclusively as a foreign key.

**Oct/Nov 2011**

**63.** Read the following statements regarding anomalies in unnormalized databases:
I Update anomaly can lead to a single real-world entity having conflicting data across multiple rows.
II Insert anomaly occurs when new data cannot be added because a required field belonging to another entity does not allow nulls.
III Delete anomaly occurs when deleting a record representing one entity unintentionally deletes information about another independent entity.
Which of the statements are correct?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) (I), (II), and (III)

**May/June 2007**

**64.** The following question consists of two statements — Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): To make an employee address table with transitive dependencies comply with 3NF, the table must be broken into two separate tables, such as employee table and employee_ zip table.
Reason (R): 3NF requires the removal of transitive functional dependencies of non-prime attributes on any super key.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2021**

**65.** The following question consists of two statements — Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): By default, a Primary Key is a clustered index, and data in the database table is physically organized in the sequence of this clustered index.
Reason (R): Every Candidate Key present in a table must be physically organized as a clustered index to maintain First Normal Form.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Downloaded from www.pdf.tube

a feature difficult to ensure in conventional file processing systems?
(A) Concurrency
(B) Data isolation
(C) Redundancy
(D) Atomicity

May/June 2025

**116.** Read the following statements regarding database design for analytical purposes:
I It is better to store all relevant data pertaining to an object along the same row.
II Storing data along the same row ensures data is easily available and optimizes read speed.
III Analytics works on historical data which is updated frequently, requiring strict 5NF compliance.
Which of the statements are correct?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) (I), (II), and (III)

Oct/Nov 2005

**117.** Which of the following is NOT an anomaly solved by database normalization?
(A) Insert anomaly
(B) Delete anomaly
(C) Update anomaly
(D) Procedural anomaly

May/June 2006

**118.** Read the following statements about Oracle Forms and Triggers:
I In a form, parent-child relationships can be maintained, known as master-detail form.
II Validation checks can be added to fields, rows, or records in a table via triggers.
III Triggers cause activation of code after an event, such as clicking a push button.
IV Triggers can only be defined at the database administrator level, never at the form or report level.
Which of the given statements are correct?
(A) Only (I), (II), and (IV)
(B) Only (I), (II), and (III)
(C) Only (II), (III), and (IV)
(D) All of the above

Oct/Nov 2024

**119.** Identify the incorrect statement regarding a Super Key.
(A) The minimal super key is known as the candidate key.
(B) It identifies uniquely rows/tuples in a table of a database.
(C) It is a combination of fields by which the row is uniquely identified.
(D) It can only ever contain a single attribute without any extra attributes.

May/June 2014

**120.** A developer uses Oracle Forms to create an application. To ensure that an employee's age entered into a text field is strictly over 18, the developer writes a piece of code that activates immediately after the user tabs out of the age field. This functionality is achieved using which of the following?
(A) A Trigger
(B) A Data Pump command
(C) A master-detail relationship
(D) An Invisible index

NODIA

Oct/Nov 2013

**121.** Read the following statements about a Database Administrator (DBA):
I The DBA centralizes the control over the data and the programs in the DBMS.
II The DBA decides what information is to be kept in the database at the logical level.
III The DBA must be aware of certain details of the physical organization of the data.
IV The DBA creates database scheme definitions which are stored permanently in the data dictionary.
Which of the statements are correct?
(A) Only (I), (II), and (IV)
(B) Only (II), (III), and (IV)
(C) Only (I), (III), and (IV)
(D) All of the above

May/June 2022

**122.** Read the following statements regarding PL/SQL:
I It includes procedural constructs such as variable declaration and conditional control.
II It excludes the ability to handle exceptions or loop constructs.
Which of the statements is/are correct?
(A) Only (I)

Which combination of statements is correct?
(A) Only (I), (II), (III), and (IV)
(B) Only (II), (III), (IV), and (V)
(C) Only (I), (III), (IV), and (V)
(D) All of the above

**Oct/Nov 2005**

**75.** Which statement correctly identifies why BCNF is referred to as 3.5NF?
(A) A bridge between physical and logical data.
(B) A requirement to denormalize into 3 tables.
(C) A theory proposed chronologically before 3NF.
(D) A stricter and more advanced version of the 3NF.

**May/June 2006**

**76.** Which of the following statements correctly identifies the types of anomalies that occur when a database is not normalized?
(A) Abstraction, view, and logical anomalies.
(B) Isolation, durability, and consistency anomalies.
(C) Procedural, embedded, and structured anomalies.
(D) Insertion, update, and deletion anomalies.

**Oct/Nov 2024**

**77.** A company table has columns: emp_id, emp_name, emp_zip, emp_state, emp_city, emp_district. The attributes emp_state, emp_city, and emp_district depend on emp_zip. The attribute emp_zip depends on emp_id. This makes the non-prime attributes transitively dependent on the super key emp_id. This structure violates:
(A) 1NF
(B) 2NF
(C) 5NF
(D) 3NF

**May/June 2014**

**78.** Who proposed the theory of normalization with the introduction of the First Normal Form?
(A) Raymond F. Boyce
(B) Charles Babbage
(C) Alan Turing
(D) Edgar Codd

**Oct/Nov 2013**

**79.** A school database table has columns: teacher_id, subject, and teacher_age. The Candidate Key is {teacher_id, subject}. The non-prime attribute teacher_age depends entirely on teacher_id alone. Which normal form does this violate?
(A) 1NF
(B) 2NF
(C) BCNF
(D) 4NF

**May/June 2022**

**80.** A company table stores employee details. Employee Jai has two mobile numbers, 8812121212 and 9900012222, stored together in a single field called emp_mobile. Which normal form rule is violated by this design?
(A) Second Normal Form (2NF)
(B) Third Normal Form (3NF)
(C) Boyce-Codd Normal Form (BCNF)
(D) First Normal Form (1NF)

**Oct/Nov 2008**

**81.** A company table stores emp_id, emp_nationality, emp_dept, dept_type, and dept_no_of_emp with functional dependencies emp_id → emp_nationality and emp_dept → {dept_type, dept_no_of_emp}. Read the following statements regarding the decomposition of this table to comply with BCNF:
I emp_nationality table with candidate key emp_id.
II emp_dept table with candidate key emp_dept.
III emp_dept_mapping table with candidate keys {emp_id, emp_dept}.
IV A generic data model table containing all attributes redundantly.
V An SDM table using domains instead of candidate keys.
Which combination of statements correctly represents the decomposed BCNF tables?
(A) Only (I), (II), and (III)
(B) Only (II), (III), and (V)
(C) Only (I), (II), and (III)
(D) Only (III), (IV), and (V)

**May/June 2007**

**82.** A company decides to close department D890. In the unnormalized employee table, Malini is the only employee assigned to D890. Deleting the records for department D890 results in the complete loss of Malini's employee information. This is an example of:
(A) Delete anomaly
(B) Insert anomaly

Click Here to Buy book on Amazon

(C) Update anomaly
(D) Isolation anomaly

Oct/Nov 2015

**83.** Which of the following is NOT true regarding the concepts of keys in normalization?
(A) A Super Key is a combination of fields by which a row is uniquely identified.
(B) A Candidate Key is the minimal Super Key from which no more attributes can be pruned.
(C) A Primary Key uniquely identifies a record in the table.
(D) A table can have multiple Primary Keys simultaneously active.

May/June 2023

**84.** Identify the correct pair representing the required conditions for a table to be in Third Normal Form (3NF).
(A) 1NF compliance without non-atomic attributes.
(B) 3NF compliance with multiple multivalued dependencies.
(C) 2NF compliance without transitive dependencies.
(D) 4NF compliance without record loss upon joining.

Oct/Nov 2018

**85.** The following question consists of two statements — Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): A table storing two mobile numbers for a single employee in one cell violates 1NF.
Reason (R): First Normal Form mandates that each attribute of a table must have atomic (single) values.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2016

**86.** A manufacturing company stores employee details and department assignments in a single table. Employee Krish belongs to two departments, resulting in two rows. If Krish's address changes, updating it in only one row results in the database showing two different addresses for Krish. What type of anomaly is this?
(A) Insert anomaly
(B) Update anomaly
(C) Delete anomaly
(D) Atomicity anomaly

Oct/Nov 2022

**87.** Which condition is the most appropriate defining rule for Boyce-Codd Normal Form (BCNF)?
(A) 2NF compliance where atomic values are absent.
(B) 3NF compliance where determinants are keys.
(C) 4NF compliance where multivalued items remain.
(D) A total restriction of all foreign key links.

NODIA

May/June 2015

**88.** What happens to the structure of a database as the normalization process sequentially upgrades from 1NF to 2NF, and then to 3NF?
(A) The number of tables decreases, and reference keys are eliminated.
(B) The number of tables and reference keys keep increasing.
(C) The database consolidates into a single flat file.
(D) The database drops all candidate keys in favor of a generic model.

Oct/Nov 2009

**89.** Consider the decomposition of the school table (teacher_id, subject, teacher_age) to comply with 2NF. Read the following statements regarding the decomposition:
I A teacher_details table containing teacher_id and teacher_age.
II A teacher_subject table containing teacher_id and subject.
III A teacher_age table containing subject and teacher_age.
IV A flat table merging teacher_id, subject, and teacher_age into atomic values.
Which of the statements is/are correct for the 2NF decomposition?
(A) Only (I) and (II)

(B) Only (III) and (IV)
(C) Only (I) and (III)
(D) Only (II) and (IV)

May/June 2010

**90.** What is the fundamental rule for a table to comply with First Normal Form (1NF)?
(A) An attribute (column) of a table cannot hold multiple values; it should hold only atomic values.
(B) No non-prime attribute is dependent on a proper subset of any candidate key.
(C) Transitive functional dependency of non-prime attributes must be removed.
(D) It must not contain more than one multivalued dependency.

Oct/Nov 2007

**91.** Match the Oracle development tool in List I with its function in List II and choose the correct option.
List I: (Oracle development tool)
P. Forms
Q. Menu
R. Oracle Report
S. Triggers
List II: (Function)
1. Produces a formatted output with nesting and subtotals.
2. Provides popup, pull down menus, and standard options like cut, paste.
3. Causes activation of a sequence of code after some specific event takes place.
4. Used for creating and running custom designed interface for querying, updating, and deleting.
(A) P-4, Q-2, R-1, S-3
(B) P-1, Q-3, R-4, S-2
(C) P-2, Q-4, R-3, S-1
(D) P-3, Q-1, R-2, S-4

May/June 2024

**92.** Which statement correctly describes Embedded DML?
(A) A query language used for interface designs.
(B) SQL used within languages like C and COBOL.
(C) A subset of DDL used to delete table files.
(D) A Hadoop command for managing HDFS blocks.

Oct/Nov 2014

**93.** What is the most appropriate condition that must be met for a table to be in 5th Normal Form (5NF)?
(A) Allowing transitive links for read speed.
(B) Converting tables into generic data models.
(C) Ensuring re-joins create no new records.
(D) Storing multiple data items in one column.

May/June 2012

**94.** Which of the following is NOT related to the ACID properties of a relational database?
(A) Atomicity
(B) Consistency
(C) Automatic indexation
(D) Isolation

Oct/Nov 2016

**95.** The following question consists of two statements — Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): The letter 'i' in Oracle 8i and 9i stands for 'Internet', as it was used to create databases for web applications.
Reason (R): The letter 'g' in Oracle 10g and 11g stands for 'grid' or 'grid computing'.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2019

**96.** When working with Oracle development tools, what is the most appropriate mechanism to activate a sequence of code after a user changes a radio button?
(A) DDL execution
(B) Trigger
(C) Materialized View
(D) Data Pump

Oct/Nov 2006

**97.** A college table contains three independent elements: college courses, the lecturer in charge of the course, and the recommended book for the course. Changing the recommended book has no effect on the course itself. Thus, the

NODIA

# ANSWERS

1. (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Conventional file systems lack centralized control to manage transactions across multiple files simultaneously. This failure often results in partial updates, which violates the principle of atomicity. Database systems solve this by ensuring that complex operations either complete fully or revert entirely, maintaining data integrity during system crashes or unexpected process interruptions.

2. (C) Relationship
An entity-relationship model represents real-world objects as entities and their associations as relationships. These relationships define how different entities interact or relate to each other logically within the database structure. For instance, a student entity might have a relationship with a course entity, illustrating enrollment as a specific logical link.

3. (C) Higher costs and potential data inconsistency.
Redundant data occurs when the same information is stored in multiple locations unnecessarily. This leads to higher storage expenses and increases the risk of inconsistency. If information is updated in one file but forgotten in another, the system provides conflicting reports, undermining the reliability and accuracy of the stored business data.

4. (C) Name, age, class
Entities in a database are described by specific properties known as attributes. For a student entity, relevant attributes include identifiable characteristics like names, ages, and grade levels. These details define the data stored about each specific instance of a student, allowing for structured organization and efficient retrieval of individual records.

5. (B) View level - Describes only a part of the entire database for a specific user.
Data abstraction simplifies user interaction by hiding complex implementation details. The view level is the highest stage, presenting specific users with only the data relevant to their needs. This approach enhances security and usability by masking the underlying physical and logical complexities, ensuring that different user groups see customized perspectives.

6. (B) Storage structure and access method
A database administrator manages the technical aspects of data organization. This includes defining physical storage structures and choosing efficient access methods to optimize performance. By determining how data is physically arranged on disk and accessed by the system, the administrator ensures rapid retrieval and reliable storage for all database operations.

7. (B) A system for managing interrelated data and programs.
A database management system acts as a software layer that controls the creation, maintenance, and use of a database. It enables users to store interrelated data efficiently while providing programs to manipulate that data. This centralized approach prevents redundancy and ensures data security, integrity, and accessibility for various applications.

8. (B) P-3, Q-2, R-1, S-4
Different levels of abstraction serve distinct purposes in a database system. The physical level describes the actual storage on disk, while the logical level defines data relationships. The view level presents specific subsets of data to users. Together, these layers facilitate data abstraction, hiding complex implementation details from end-users.

9. (D) They complicate data exchange and data integration by avoiding standardization.
Generic data models are designed to improve data exchange and integration by providing standardized, general relation types. They address the limitations of conventional models by offering a flexible framework for representing diverse information. By utilizing generalizations,

Downloaded from www.pdf.tube

Which combination of statements is correct?
(A) Only (I), (II), (IV), and (V)
(B) Only (I), (III), (IV), and (V)
(C) Only (II), (III), (IV), and (V)
(D) All of the above

**Oct/Nov 2011**

**105.** What is the most appropriate description of a Foreign Key?
(A) A unique key that holds multiple atomic data values in one field.
(B) A field in a table that is a Primary Key in another table.
(C) An attribute that is restricted from holding data type definitions.
(D) A key used to restrict the database to First Normal Form only.

**May/June 2007**

**106.** Identify the incorrect statement regarding 4NF and 5NF.
(A) A model that builds on the first three forms and BCNF.
(B) The most common form in commercial use.
(C) A rule against multiple multivalued items.
(D) A state where re-joins do not lose records.

**Oct/Nov 2021**

**107.** Which of the following is NOT a capability of Oracle Report 10g?
(A) Managing physical disk fragmentation levels.
(B) Creating multiple breaks on data columns.
(C) Generating grand totals with page formatting.
(D) Providing subtotals and page numbering.

**May/June 2013**

**108.** Which of the following correctly describes the responsibilities of the Oracle kernel part?
(A) Storage, access, backup, and recovery.
(B) Designing forms and graphical menus.
(C) Providing redundancy for NoSQL systems.
(D) Executing COBOL without using any SQL.

**Oct/Nov 2017**

**109.** Identify the incorrect statement about the DBA function “Scheme definition”.
(A) The initial creation of the database system.
(B) Storing definitions within the dictionary.
(C) Control by the database administrator.
(D) Defining rotation speeds of physical disks.

**May/June 2009**

**110.** A database administrator needs to enhance the export and import of large volumes of data securely. They utilize a feature in Oracle 11g that supports encryption and compression options. Which command or tool are they using?
(A) PL/SQL Exception Handler
(B) Oracle Menu builder
(C) Data Pump command
(D) Materialized View logs

**Oct/Nov 2012**

**111.** What is the most appropriate goal of Data Abstraction?
(A) Exposing all hardware details to users.
(B) Increasing redundancy across the tables.
(C) Enforcing consistency in NoSQL systems.
(D) Hiding details to simplify interaction.

NODIA

**May/June 2011**

**112.** Oracle 21c is a database cloud service. What does the letter ‘c’ stand for in this version?
(A) Computing
(B) Cloud
(C) Concurrent
(D) Cluster

**Oct/Nov 2020**

**113.** Identify the incorrect statement regarding Third Normal Form (3NF).
(A) A table must first be in 2NF.
(B) An attribute that is a part of the candidate key is known as a non-prime attribute.
(C) Transitive functional dependency of non-prime attributes on any super key should be removed.
(D) If $X \rightarrow Y$, X is a super key of the table and Y is a prime attribute of the table are conditions related to 3NF.

**May/June 2017**

**114.** Which of the following is NOT a feature introduced or improved in Oracle 11g compared to 10g?
(A) Invisible indexes
(B) Virtual columns
(C) Elimination of the Data Pump command
(D) Table partitioning

**Oct/Nov 2019**

**115.** Which property dictates that a set of commands should be applied comprehensively or not at all,

course depends on both lecturer and book. This is an example of:
(A) Transitive dependency
(B) Atomic dependency
(C) Clustered index dependency
(D) Multivalued dependency

**May/June 2020**

**98.** Match the Oracle version in List I with its corresponding descriptive letter meaning in List II and choose the correct option.
List I: (Oracle version)
P. Oracle 8i
Q. Oracle 10g
R. Oracle 21c
S. Oracle 11g
List II: (Descriptive letter meaning)
1. Grid computing
2. Internet
3. Cloud
4. Grid
(A) P-2, Q-4, R-3, S-1
(B) P-1, Q-2, R-4, S-3
(C) P-3, Q-1, R-2, S-4
(D) P-4, Q-3, R-1, S-2

**Oct/Nov 2010**

**99.** Identify the incorrect statement about the Primary Key.
(A) Unique identification of a record in a table.
(B) A table with multiple primary keys active.
(C) Defaulting to a clustered index structure.
(D) Physical data organization by index sequence.

**May/June 2005**

**100.** Identify the incorrect statement regarding PL/SQL provided by Oracle.
(A) It includes procedural constructs such as conditional control.
(B) It includes loop constructs.
(C) It is purely a non-procedural query language without variable declaration.
(D) It includes exception handling and relational statements.

**Oct/Nov 2025**

**101.** Read the following statements regarding Oracle's SQL support:
I Oracle supports standard SQL commands like select, insert, create, and delete.
II Oracle supports set operators such as union, intersect, and minus.
Which of the statements is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**May/June 2018**

**102.** Match the Normal Form in List I with its core condition in List II and choose the correct option.
List I: (Normal Form)
P. 1NF
Q. 2NF
R. 3NF
S. BCNF
List II: (Core condition)
1. Transitive functional dependency of non-prime attribute on any super key is removed.
2. For every functional dependency $X \rightarrow Y$, X should be the super key.
3. Attribute cannot hold multiple values; atomic values only.
4. No non-prime attribute is dependent on the proper subset of any candidate key.
(A) P-3, Q-4, R-1, S-2
(B) P-4, Q-3, R-2, S-1
(C) P-1, Q-2, R-3, S-4
(D) P-2, Q-1, R-4, S-3

**Oct/Nov 2023**

**103.** Which statement correctly identifies the problem of "Data isolation" in a file processing system?
(A) Data centralized in single table files.
(B) Data scattered in various file locations.
(C) Data requiring triggers for isolation.
(D) Data accessed only by the administrator.

**May/June 2008**

**104.** Read the following statements comparing Oracle 11g to 10g:
I 11g provides more simplified, improved, and automated memory management.
II 11g has a better ability to diagnose faults through an inbuilt infrastructure.
III 11g lacks the ability to redefine tables which have materialized view logs whilst online.
IV 11g introduces better password-based authentication with mixed case passwords.
V 11g includes encryption on the table-space level.

Click Here to Buy book on Amazon

(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**Oct/Nov 2008**

**123.** The following question consists of two statements — Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): A table containing a college course, the lecturer, and the recommended book (where lecturer and book are independent of each other) contains a multivalued dependency.
Reason (R): Fourth Normal Form (4NF) states that a table should not have more than one multivalued dependency.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2010**

**124.** Read the following statements regarding the Oracle kernel:
I It handles the definition and storage of data.
II It manages database access control and concurrent access handling.
III It interprets SQL statements and provides backup and recovery of the database.
Which of the statements are correct?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) (I), (II), and (III)

**Oct/Nov 2015**

**125.** Read the following statements about Relational DBMS (RDBMS):
I They are powerful because they require few assumptions about how data is related.
II A single database can be spread across several tables.
III Normalization eliminates the need to redundantly store related data in multiple tables.
IV Normalization streamlines database maintenance and enables faster querying.
V Normalization is a concept that applies strictly to NoSQL file-based databases.
Which combination of statements is correct?
(A) Only (I), (II), (III), and (IV)
(B) Only (II), (III), (IV), and (V)
(C) Only (I), (III), (IV), and (V)
(D) All of the above

www.nodia.in

NODIA

May/June 2013

**66.** A company table stores emp_id, emp_nationality, emp_dept, dept_type, and dept_no_of_emp. Functional dependencies are:
- emp_id → emp_nationality
- emp_dept → {dept_type, dept_no_of_emp}

The Candidate key is {emp_id, emp_dept}. Neither emp_id nor emp_dept alone are keys. This table violates which normal form directly addressing functional dependencies on non-super keys?
(A) BCNF
(B) 1NF
(C) 2NF
(D) 5NF

Oct/Nov 2017

**67.** What is the primary purpose of normalization in a database?
(A) Merging tables into large files for speed.
(B) Processing data within Hadoop environments.
(C) Organizing data to avoid logic anomalies.
(D) Ensuring consistency in NoSQL environments.

May/June 2009

**68.** Identify the incorrect pair regarding Normal Forms and their conditions.
(A) 1NF - Attributes must hold only atomic values.
(B) Table is in 2NF and no non-prime attribute is dependent on the proper subset of any candidate key.
(C) 3NF - Table is in 2NF and contains multiple non-trivial multivalued dependencies.
(D) BCNF - For every functional dependency X → Y, X should be the super key.

Oct/Nov 2012

**69.** Boyce-Codd Normal Form (BCNF) is an advanced, stricter version of which Normal Form?
(A) 3NF
(B) 1NF
(C) 2NF
(D) 4NF

May/June 2011

**70.** Which of the following represents the correct chronological evolution of Normalization theories as proposed by Edgar Codd and Raymond F. Boyce?
(A) 1NF → 2NF → BCNF → 3NF
(B) 1NF → 2NF → 3NF → BCNF
(C) 1NF → 3NF → 2NF → BCNF
(D) BCNF → 1NF → 2NF → 3NF

Oct/Nov 2020

**71.** What defines a multivalued dependency in the context of Fourth Normal Form (4NF)?
(A) Dependence on multiple independent values.
(B) Primary keys holding multiple null values.
(C) Columns holding non-atomic data strings.
(D) Attributes depending on candidate key subsets.

May/June 2017

**72.** A new trainee joins a company but is not yet assigned to any department. The single employee table requires a department value and does not allow nulls in the emp_dept field. Consequently, the trainee cannot be added to the database. This scenario illustrates which anomaly?
(A) Update anomaly
(B) Insert anomaly
(C) Delete anomaly
(D) Redundancy anomaly

Oct/Nov 2019

**73.** For a table to be in Second Normal Form (2NF), which of the following conditions is most appropriate?
(A) 1NF compliance without transitive dependencies.
(B) Each determinant functioning as a candidate key.
(C) Prevention of more than one multivalued dependency.
(D) 1NF compliance without partial dependencies.

May/June 2025

**74.** Read the following statements about keys:
I A Candidate Key can be a combination of columns.
II There can be multiple Candidate Keys in one table.
III Each Candidate Key can qualify as a Primary Key.
IV A Primary Key can be only one for a given table.
V A Foreign Key is a field in the table that is a Primary Key in another table.

Downloaded from www.pdf.tube

these models simplify the process of merging data from different sources into a unified system.

10. (A) Only (I)
File processing systems often suffer from data isolation because information is stored in various files with different formats across separate locations. This makes it difficult to retrieve combined data or ensure consistency. However, resolving integrity problems is not easy in these systems, as new constraints require complex modifications to multiple application programs.

11. (A) P-4, Q-2, R-3, S-1
The database administrator performs several critical roles to maintain a healthy system. These include defining the database scheme, granting access permissions to authorized users, and specifying integrity constraints to ensure data accuracy. Additionally, the administrator creates efficient storage structures and access methods to optimize how the system handles various data requests.

12. (C) Environments allow needed data to be retrieved in a convenient and efficient manner.
File processing systems are characterized by several significant drawbacks, including data redundancy and difficulty in enforcing consistency constraints. These systems lack the sophisticated query mechanisms found in modern databases, making data retrieval inconvenient and inefficient. Managing concurrent access by multiple users also presents a major challenge, often leading to conflicting updates.

13. (A) Flat data-model
The flat data model is considered the simplest and earliest form of data organization. In this model, all data elements are kept in a single, two-dimensional plane, much like a spreadsheet. It lacks the complex relational links and hierarchical structures found in more modern models, making it suitable only for very simple data storage requirements.

14. (C) Physical level
The physical level of data abstraction focuses on the lowest tier of the system architecture. It describes in detail how data is actually stored on storage devices and manages complex data structures. This level is concerned with efficiency and technical implementation, which are usually hidden from the end-users and programmers by the DBMS.

15. (A) P-3, Q-2, R-4, S-1
Mapping cardinality expresses the number of entities to which another entity can be associated via a relationship set. Common types include one-to-one, one-to-many, many-to-one, and many-to-many. These definitions are crucial for designing accurate entity-relationship models, as they reflect the real-world constraints and connections between different types of data in the system.

16. (A) Hadoop Distributed File System (HDFS)
Hadoop relies on the Hadoop Distributed File System to manage massive amounts of data across multiple servers. This architecture provides high-speed access and fault tolerance by distributing data blocks across the cluster. It serves as the foundational bedrock for big data processing, allowing for scalable storage and efficient parallel computing in large enterprises.

17. (C) Assertion (A) is true, but Reason (R) is false.
A semantic data model treats entities as whole objects, preserving their conceptual meaning without breaking them into smaller table fragments immediately. This approach focuses on how data relates to real-world concepts. In contrast, relational models often normalize data by splitting it into multiple tables, which can sometimes lose the immediate conceptual clarity of the entity.

18. (A) Hadoop File System (HDFS)
Big data environments often face challenges with isolated and scattered files across massive server clusters. The Hadoop Distributed File System addresses this by providing a unified, scalable storage layer. This technology allows structured and unstructured data to be managed as a single logical unit, facilitating easier access and processing across thousands of server nodes.

19. (D) Defining a table as an n-ary relation via logic.
The relational model organizes data into tables, which are mathematically defined as n-ary relations. This logical structure allows for data to be manipulated using relational algebra and calculus. Each row in a table represents

NODIA

**79.** (B) 2NF
In this example, the candidate key is a combination of teacher ID and subject. The teacher's age depends only on the teacher ID, which is a proper subset of the key. This partial dependency violates Second Normal Form, which mandates that every non-prime attribute must depend on the whole candidate key. Teacher details should be moved.

**80.** (D) First Normal Form (1NF)
First Normal Form requires that every attribute in a table must hold only atomic, or single, values. Storing two mobile numbers in one field violates this rule because the data is not broken down into its simplest form. To correct this, the designer should either create a new row for each number or move them to a separate table.

**81.** (A) Only (I), (II), and (III)
To reach Boyce-Codd Normal Form, a table must be decomposed such that every functional dependency has a super key as its determinant. This involves splitting the original table into three separate entities: one for nationality, one for department details, and a mapping table to link employees to their departments. This structure eliminates redundancy and ensures valid dependencies.

**82.** (A) Delete anomaly
A delete anomaly occurs when removing one piece of information from a table unintentionally results in the loss of other, unrelated information. In this scenario, closing a department leads to the deletion of an employee's record because the data was not properly normalized into separate tables. This highlights the importance of separating different entities into their own tables.

**83.** (D) A table can have multiple Primary Keys simultaneously active.
While a table can have several candidate keys, only one can be designated as the primary key. The primary key serves as the main unique identifier for each record. Other properties of keys include super keys being combinations for identification and candidate keys being minimal versions. Having multiple primary keys would create unnecessary complexity in identifying data records.

**84.** (C) 2NF compliance without transitive dependencies.
Third Normal Form represents a stage of database refinement where a table must already meet the criteria for Second Normal Form. The additional requirement for 3NF is the removal of all transitive functional dependencies. This ensures that every non-prime attribute depends only on the primary key, rather than on other non-prime attributes, which further reduces data redundancy.

**85.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
First Normal Form is the most basic level of normalization, requiring all table attributes to contain only atomic values. When multiple phone numbers are stored in a single cell, the data is not atomic, directly violating this rule. Ensuring atomicity simplifies data manipulation and allows the database engine to perform searches and updates more effectively on individuals.

**86.** (B) Update anomaly
An update anomaly occurs when data is duplicated across multiple rows, and a change to that information is not applied consistently to all instances. In this case, updating Krish's address in one row but not the other results in conflicting data. Normalization prevents this by ensuring that the address is stored in only one location for each employee.

**87.** (B) 3NF compliance where determinants are keys.
Boyce-Codd Normal Form is a strict version of the third normal form. It adds the requirement that for every non-trivial functional dependency, the determinant must be a super key. This rule ensures that all dependencies are based on the unique identifiers of the table, eliminating the possibility of anomalies related to overlapping candidate keys that 3NF might miss.

**88.** (B) The number of tables and reference keys keep increasing.
As a database moves through the normalization process from 1NF to 3NF, the designer decomposes large, complex tables into smaller, more specialized ones. This reduces redundancy but increases the total number of tables in the

Click Here to Buy book on Amazon

# STUDYING FROM PDFs?

# THINK AGAIN.

If you are studying only from PDFs,
you are wasting valuable time.

Research shows that learning from

**PRINTED BOOKS** has up to

**4× HIGHER RETENTION**

than studying from screens.

**PRINT BOOK = BETTER MEMORY**

**PDF = LOWER RETENTION**

Those who study from **PRINTED BOOKS**
move **AHEAD.**

Others are left **BEHIND**
in competition.

In competitive exams,
being average is not enough.

## STAY ONE STEP AHEAD.

different rows or tables to maintain the integrity and simplicity of the stored relations.

**30.** (A) Only (I) and (II)
The logical level of abstraction is used by administrators to define the database's content and structure. The physical level describes complex, low-level data structures in detail. Conversely, the view level is designed to show only a subset of the database to specific users, rather than forcing everyone to see the entire database concurrently during interaction.

**31.** (C) Primary Key
A primary key is a unique identifier chosen by the database designer to distinguish each record in a table. In an employee table, the employee number serves this purpose because it is unique to every individual and cannot be repeated. This ensures that every row can be accessed and updated accurately without any possible ambiguity.

**32.** (C) Assertion (A) is true, but Reason (R) is false.
A view is a virtual table that allows users to see a restricted or simplified portion of the database. While it can provide access to complex underlying data structures, it does not physically duplicate the data. Instead, a view is essentially a saved query that retrieves data from base tables whenever the view is accessed.

**33.** (B) A single relational database can be spread across several tables.
Relational databases differ from flat-file systems because they organize data into multiple related tables rather than a single large file. This structure allows for normalization, which reduces redundancy and improves data integrity. By using keys to link tables, relational systems can manage complex data relationships more efficiently than traditional isolated flat files.

**34.** (D) Guarantees total correctness of applications.
The consistency property in ACID ensures that a transaction takes the database from one valid state to another, following all defined rules and constraints. While it enforces data integrity through triggers and cascades, it cannot guarantee the absolute correctness of the application logic itself. It only ensures that database-level rules are strictly followed.

**35.** (A) isolate
Standard SQL queries are built using several fundamental clauses that define the operation. The select clause identifies the attributes to retrieve, the from clause specifies the tables to scan, and the where clause sets the filtering conditions. The term "isolate" is a property of transactions rather than a clause used in the SQL query language.

**36.** (A) Durability
Durability ensures that once a transaction is committed, its effects are permanently recorded in non-volatile memory. This property guarantees that the data will survive even in the event of a system crash or power failure. By writing changes to disk, the database ensures the integrity of committed transactions remains intact during the restoration process.

**37.** (A) Attributes that collectively identify an entity.
A super key is a set of one or more attributes that, taken together, allow the system to uniquely identify a record in a table. It provides the basis for defining candidate keys and primary keys. While a super key can include extra attributes, its core function is to ensure that no two rows in the table are identical.

**38.** (D) select empno, empname from emp where empjoin > '01-DEC-09'
To retrieve specific information from a database, the select clause lists the desired columns, such as employee number and name. The from clause specifies the source table. The where clause applies a filter, using a greater-than operator with the specified date to identify employees who joined the company after the given chronological timeframe.

**39.** (D) NoSQL databases
Many NoSQL databases are designed for high availability and scalability, often relaxing strict ACID requirements. Instead, they provide eventual consistency, where data updates eventually propagate to all nodes in a distributed system. This approach is common in large-scale environments where immediate synchronization across thousands of servers is technically challenging or impacts system performance.

Downloaded from www.pdf.tube

a unique record, and each column contains values belonging to a specific domain, ensuring a structured approach to data management.

**20.** (A) Logical level
When a database administrator defines the relationships between entities like customers and transactions without worrying about physical storage, they are working at the logical level. This level describes what data is stored and the connections between them. It provides a blueprint of the database structure that is independent of specific hardware implementation details.

**21.** (C) Granting of authorization - Maintaining data consistency across atomic values.
Granting authorization is the process of providing specific users with permission to access or modify data. It is a security function rather than a consistency check. Maintaining data consistency through constraints is part of the integrity constraints specification function, which ensures that all data values adhere to the rules defined by the system designer.

**22.** (B) Automatic data indexation
File processing systems typically lack automated features such as data indexation, which makes searching for information slow and manual. In contrast, modern database systems use automatic indexing to speed up retrieval. The main disadvantages of file systems include data isolation, difficulty in managing concurrent access, and various data integrity and security problems that arise.

**23.** (D) Hiding storage details to simplify interaction.
Data abstraction is a fundamental principle in database design that involves hiding the complex details of how data is stored and maintained. By presenting users with a simplified view of the data, the system becomes easier to use and more accessible. This allows developers and users to focus on the logical information requirements.

**24.** (A) Only (I), (II), and (III)
The semantic data model focuses on the meaning of data and its interrelationships within a real-world context. It defines how stored symbols relate to physical objects. In this model, an entity behaves similarly to a domain. Unlike normalized relational models, SDM avoids breaking entities into multiple tables to maintain their original conceptual integrity.

**25.** (B) How the logical structure of a database is modelled and how data is connected.
Data models provide the conceptual framework for organizing data in a database management system. They define the logical structure, the relationships between different data elements, and the constraints that ensure data integrity. By using a data model, designers can create a clear and consistent representation of the information required for a specific application.

**26.** (D) Transactions applied completely or not at all.
Atomicity is a core property of database transactions ensuring that all operations within a single unit of work are performed successfully. If any part of the transaction fails, the entire transaction is rolled back, leaving the database unchanged. This "all or nothing" approach prevents partial updates, which would otherwise lead to inconsistent or corrupted data.

NODIA

**27.** (A) An object instance providing specific details.
In a semantic data model, values within a domain act as pointers to specific object instances. These instances represent real-world entities and provide detailed information about them. This structure allows the system to maintain the meaning of data by linking individual names or identifiers directly to the objects they represent in the logical data model.

**28.** (A) P-3, Q-2, R-1, S-4
File processing systems face several significant challenges that hinder efficient data management. Data redundancy leads to increased storage costs and potential inconsistencies. Integrity problems arise when constraints across different files are hard to enforce. Concurrency issues occur when multiple users update data simultaneously without supervision, and security problems involve limited access control mechanisms.

**29.** (C) Saving multi-valued data in normalized relations.
A key rule of the relational model, specifically in the context of first normal form, is that attributes must contain only atomic values. This means multi-valued data is not allowed within a single cell. Instead, such data must be separated into

**50.** (C) Displays the empcity attribute for all records.
The select clause identifies the specific column to be retrieved, which is “empcity” in this case. The from clause identifies the target table, “emp”. When executed, the query will return a list showing the values stored in the city attribute for every row currently present in the employee table, without modifying any structural data.

**51.** (A) Processing concurrent tasks as if sequential.
The isolation property ensures that even when multiple transactions occur at the same time, the final state of the database is as if they were executed one after another. This prevents conflicts, such as two people booking the same seat. It maintains data integrity by keeping the intermediate states of transactions invisible to other concurrent processes.

**52.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
A primary key must uniquely identify each row in a table. Since null values represent unknown or missing data, allowing them would create ambiguity and prevent the system from distinguishing between records. Therefore, designers must ensure that primary key columns are always populated with unique, valid values to maintain the structural integrity of the database.

**53.** (C) Users specifying a manual sequence of operations.
SQL is primarily a non-procedural language, meaning users describe what data they want rather than specifying the exact sequence of steps to retrieve it. While it can be embedded in procedural languages like C, the core SQL commands for data manipulation and definition focus on set-based operations where the database engine determines the execution path.

**54.** (D) All of the above
Database technology encompasses various architectures, each with specific features. Relational systems use schemas, primary keys, and normalization to manage data consistently. NoSQL systems were developed to offer more flexibility than the rigid relational model. Additionally, big data solutions like Hadoop utilize distributed file systems to handle massive volumes of information across many different server nodes.

**55.** (A) P-4, Q-3, R-2, S-1
SQL is divided into several sub-languages with specific roles. Data Definition Language is used to manage table structures, while Data Manipulation Language handles the data within those tables. In a query, the select clause identifies the desired attributes, and the from clause lists the source tables. These components work together to provide a comprehensive database language.

**56.** (A) Only (I)
In a relational database, every attribute has a domain, which defines the set of all possible permitted values. This ensures data consistency by restricting entries to a specific type. Null values, on the other hand, represent unknown or missing information rather than a rigidly defined or known value, and their presence indicates that data is currently unavailable.

**57.** (A) Eventual consistency
ACID compliance requires strict consistency, where every transaction leaves the database in a valid state immediately upon completion. Eventual consistency is a weaker model used in many distributed NoSQL systems, where data becomes consistent across all nodes over time. The core ACID properties are atomicity, consistency, isolation, and durability, which ensure reliable and immediate transactions.

**58.** (A) Data Definition Language (DDL)
Data Definition Language consists of SQL commands used to create, modify, or delete the structures of a database, such as tables and indexes. Unlike DML, which manages the actual data records, DDL defines the schema and rules governing how data is organized. Common DDL commands include CREATE, ALTER, and DROP, which are essential for database administration.

**59.** (A) Only (I)
Relational Database Management Systems are built to support referential integrity and strict adherence to ACID properties, ensuring reliable transactions. Many NoSQL databases, however, prioritize performance and scalability over strict ACID compliance, often opting for eventual consistency models. This makes RDBMS better

Click Here to Buy book on Amazon

**98.** (A) P-2, Q-4, R-3, S-1
Oracle has historically used letters in its version numbers to highlight key technological advancements. The 'i' stands for Internet-enabled capabilities, the 'g' signifies the adoption of grid computing for distributed resource management, and the 'c' represents modern cloud-based services. Matching these letters to their meanings helps identify the technological era and primary focus of each database version.

**99.** (B) A table with multiple primary keys active.
A primary key is a unique identifier for records within a table, and by definition, a table can have only one primary key at a time. This key usually defaults to a clustered index structure, which physically organizes data on disk for faster access. While a table may have multiple candidate keys, only one is chosen as primary.

**100.** (C) It is purely a non-procedural query language without variable declaration.
PL/SQL is Oracle's procedural extension to SQL. Unlike standard SQL, which is non-procedural, PL/SQL allows for variable declarations, conditional control structures like IF statements, and loop constructs. It also includes sophisticated exception handling and allows for the integration of standard relational SQL statements within blocks of procedural code, making it a powerful tool for application developers.

**101.** (C) Both (I) and (II)
Oracle's implementation of SQL provides comprehensive support for standard commands such as SELECT, INSERT, CREATE, and DELETE for managing data and structures. Additionally, it includes powerful set operators like UNION, INTERSECT, and MINUS, which allow users to combine the results of multiple queries. This robust support ensures full compatibility with relational database standards and operations.

**102.** (A) P-3, Q-4, R-1, S-2
Each normal form addresses specific types of data redundancy and dependency. 1NF requires atomic values in every column. 2NF removes partial dependencies where non-prime attributes depend on parts of a key. 3NF eliminates transitive dependencies between non-prime attributes. BCNF is the strictest, ensuring that for every functional dependency, the determinant is a super key, providing high data integrity.

**103.** (B) Data scattered in various file locations.
Data isolation occurs in traditional file processing systems because information is often stored in separate files across various locations. These files may have different formats and are managed by different application programs. This fragmentation makes it extremely difficult to perform operations that require data from multiple sources or to ensure that data remains consistent across the environment.

NODIA

**104.** (A) Only (I), (II), (IV), and (V)
Oracle 11g introduced significant improvements over 10g, including automated memory management, a better fault diagnosis infrastructure, and enhanced security with mixed-case passwords. It also provided table-space level encryption. However, the claim that it lacks the ability to redefine tables with materialized view logs online is incorrect, as this version actually improved such online maintenance capabilities for administrators.

**105.** (B) A field in a table that is a Primary Key in another table.
A foreign key is an attribute used to create a link between two tables. It consists of a column in one table that references the primary key of another table. This mechanism is essential for maintaining referential integrity in a relational database, as it ensures that relationships between data records are consistently enforced across different system parts.

**106.** (B) The most common form in commercial use.
While higher normal forms like 4NF and 5NF provide the highest level of data integrity by eliminating multi-valued and join dependencies, they are not the most commonly used in commercial settings. Most business databases are normalized up to 3NF or BCNF, as these levels offer a practical balance between data integrity and performance costs.

**107.** (A) Managing physical disk fragmentation levels.
Oracle Report 10g is a specialized tool designed for generating formatted, professional-looking business reports from database data. It excels at tasks like creating data breaks, calculating grand

**69.** (A) 3NF
Boyce-Codd Normal Form is often referred to as a stronger version of the third normal form. It addresses specific functional dependencies that 3NF might miss, particularly when there are multiple overlapping candidate keys. For a table to be in BCNF, every determinant must be a super key, providing a more rigorous standard for eliminating redundancy.

**70.** (B) 1NF → 2NF → 3NF → BCNF
The theory of normalization evolved progressively. Edgar Codd initially proposed the first three normal forms to address basic redundancy and dependency issues. Later, in collaboration with Raymond Boyce, the Boyce-Codd Normal Form was introduced as a stricter refinement of the third normal form. This chronological sequence represents the deepening understanding of relational data structure.

**71.** (A) Dependence on multiple independent values.
A multivalued dependency occurs when one attribute in a table implies the presence of multiple values of another attribute, and these sets of values are independent of other attributes. Fourth Normal Form was designed to eliminate the redundancy caused by these dependencies. It ensures that independent many-to-many relationships are not stored in the same table.

**72.** (B) Insert anomaly
An insert anomaly happens when new data cannot be added to the database because of the absence of other unrelated data. In this case, the trainee's record cannot be created because the system requires a department assignment, which the trainee does not yet have. This is a clear sign that the table needs further normalization.

**73.** (D) 1NF compliance without partial dependencies.
For a table to reach Second Normal Form, it must first satisfy the requirements of the First Normal Form. Additionally, it must ensure that every non-prime attribute is fully functionally dependent on the entire candidate key. This means removing partial dependencies, where an attribute depends only on a portion of a composite primary key.

**74.** (D) All of the above
Candidate keys are sets of columns that uniquely identify rows and can be used as primary keys. A table can have multiple candidate keys, but only one is selected as the primary key. Foreign keys establish links between tables by referencing the primary key of another table. These various keys work together to ensure overall data integrity.

**75.** (D) A stricter and more advanced version of the 3NF.
Boyce-Codd Normal Form is colloquially known as 3.5NF because it sits between the third and fourth normal forms in terms of strictness. It applies a more rigorous rule where every determinant in a functional dependency must be a super key. This addresses certain anomalies that can still occur in 3NF tables with complex overlapping candidate keys.

**76.** (D) Insertion, update, and deletion anomalies.
Poorly designed databases often suffer from three main types of logical anomalies. Insertion anomalies prevent adding new records, update anomalies lead to data inconsistencies when changes are made, and deletion anomalies result in the loss of unrelated information. Normalization is the primary technique used by database designers to identify and resolve these critical data integrity issues.

**77.** (D) 3NF
The scenario describes a transitive dependency where state and city depend on the zip code, which in turn depends on the employee ID. This structure violates the Third Normal Form, which requires the removal of all transitive functional dependencies of non-prime attributes on any super key. To fix this, the address details should be moved to a separate table.

**78.** (D) Edgar Codd
Edgar Codd, a computer scientist at IBM, is credited with inventing the relational model for database management and the concept of normalization. He introduced the first three normal forms as a way to organize data into tables to minimize redundancy and improve integrity. His pioneering work laid the foundation for modern relational database systems used globally.

Downloaded from www.pdf.tube

**40.** (D) The user instructs the system to perform a sequence of operations.
In a procedural query language, the user specifies both what data is needed and the exact sequence of steps required to obtain it. This contrasts with non-procedural languages, where the user only describes the desired result. Procedural approaches give developers more control over the execution flow, which is useful for complex data processing.

**41.** (A) P-3, Q-4, R-2, S-1
ACID properties ensure reliable transaction processing. Atomicity requires an "all or nothing" execution. Consistency ensures the database moves between valid states. Isolation guarantees that concurrent transactions appear to run sequentially, preventing interference. Durability ensures that committed data is saved in non-volatile storage to survive crashes, maintaining the system's overall long-term integrity.

**42.** (D) (I), (II), and (III)
A super key is any set of attributes that uniquely identifies a row, often including redundant ones. A candidate key is a minimal super key with no unnecessary attributes. The primary key, chosen from the candidate keys, must not contain null values, as every record must be uniquely and reliably identifiable within the database table.

**43.** (B) Only (I), (II), and (IV)
A view is a virtual table derived from one or more base tables, providing a limited data perspective. While base tables are often physical, they can also be other views, allowing for layered data abstraction. In most cases, views are used for reading data rather than performing updates, which simplifies user interactions and enhances overall security.

**44.** (D) where
The where clause in an SQL statement is used to filter records based on specific criteria. It contains conditions involving the attributes of the tables mentioned in the from clause. Only the rows that satisfy these conditions are included in the result set, allowing users to extract precisely the information they need from the database table.

NODIA

**45.** (C) Assertion (A) is true, but Reason (R) is false.
Durability ensures that committed transaction data is preserved even during power losses or system failures. However, to achieve this, the system must record data in non-volatile memory, such as a hard drive. Volatile memory, like RAM, loses all stored information when power is cut, making it unsuitable for ensuring the durability of committed database records.

**46.** (B) A Primary Key is permitted to have multiple null values.
A primary key must uniquely identify every row in a table, which means it cannot contain any null values. Nulls represent unknown information, which would prevent the system from accurately identifying and distinguishing between records. Other key properties include the ability for super keys to have extra attributes and the designer selecting the key.

**47.** (A) Atomicity, Consistency, Isolation, Durability.
ACID is a set of properties that guarantee database transactions are processed reliably. Atomicity ensures complete execution, consistency maintains valid states, isolation prevents concurrent interference, and durability ensures that committed data survives system failures. These principles are fundamental to the design and operation of traditional relational systems, ensuring high levels of data integrity.

**48.** (B) Foreign Key
When an attribute in one table serves as the primary key for another table, it is called a foreign key. In this scenario, the "Department Number" in the "Employee" table links employees to their respective departments. This relationship allows the database to maintain data integrity and enables the efficient retrieval of related information across multiple tables.

**49.** (A) Relational databases
Normalization is a systematic process used in the design of relational databases to minimize redundancy and prevent anomalies. By organizing data into multiple related tables, it ensures that each data item is stored in only one place. This concept is central to relational theory and does not apply to flat-file or other less structured data models.

schema. Consequently, the number of foreign keys used to link these tables also increases to maintain the relationships between separated data.

**89.** (A) Only (I) and (II)
To decompose the school table into Second Normal Form, the partial dependency of age on teacher ID must be removed. This results in two separate tables: one for teacher details like age and another to map teachers to the subjects they teach. This separation ensures that every attribute is fully dependent on the primary key of its table.

**90.** (A) An attribute (column) of a table cannot hold multiple values; it should hold only atomic values.
The core requirement of First Normal Form is that each column in a table must contain only indivisible, atomic values. This means no lists, sets, or groups of data should be stored in a single cell. By enforcing atomicity, 1NF provides a uniform structure that allows for simpler query logic and more predictable data management within a database.

**91.** (A) P-4, Q-2, R-1, S-3
Oracle provides a suite of tools for application development. Forms is used for creating user interfaces, while Menu offers standard navigation options. Oracle Report generates formatted outputs like subtotals. Triggers are essential for automation, as they activate specific code sequences in response to events. These tools work together to build interactive database-driven applications for organizations.

**92.** (B) SQL used within languages like C and COBOL.
Embedded DML refers to the practice of including standard SQL data manipulation statements directly within the source code of a procedural programming language. This allows developers to combine the power of SQL's data retrieval with the complex logic and control structures of languages like C. The system uses a precompiler to translate these statements for execution.

**93.** (C) Ensuring re-joins create no new records.
Fifth Normal Form deals with cases where a table cannot be decomposed into smaller tables without losing information or creating false data upon re-joining. A table is in 5NF if every join dependency is implied by the candidate keys. This ensures that the original data can be reconstructed perfectly through join operations without any loss of integrity.

**94.** (C) Automatic indexation
ACID properties are the standard for ensuring reliable transaction processing in database systems. They consist of atomicity, consistency, isolation, and durability. While automatic indexation is a useful feature for improving the performance of data retrieval in many modern databases, it is not part of the fundamental ACID transaction model that guarantees data integrity during system operations.

**95.** (B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
Oracle used letters to denote the primary focus of different software versions. The 'i' in 8i stood for 'Internet', reflecting the shift toward web-enabled databases. The 'g' in 10g represented 'grid', focusing on grid computing. While both statements are true, the shift to grid computing is not an explanation for the earlier Internet-focused naming convention used.

**96.** (B) Trigger
A trigger is a specialized piece of code in a database or application that automatically executes in response to a specific event. In user interfaces created with tools like Oracle Forms, a trigger can be set to run when a user interacts with a control, such as clicking a radio button. This provides immediate validation and process automation.

**97.** (D) Multivalued dependency
A multivalued dependency arises when one attribute in a table determines a set of values for another attribute, and these values are independent of other data in the table. In the example, the course name determines both a lecturer and a book, but the lecturer and book are not related to each other. This requires table decomposition.

Click Here to Buy book on Amazon

suited for applications requiring high data accuracy and immediate consistency, such as financial systems.

**60.** (B) It is used to list the attributes desired in the result of the query.
The select clause is a fundamental part of an SQL query that specifies which columns or attributes should be returned in the result set. It allows users to filter vertically, choosing only the relevant fields from a table. This makes data retrieval more efficient by excluding unnecessary information from the output provided to the end user.

**61.** (A) P-4, Q-3, R-1, S-2
Database anomalies arise from poor design. An update anomaly causes inconsistencies when replicated data is only partially changed. An insert anomaly prevents adding data when some fields are missing. A delete anomaly occurs when removing one piece of information unintentionally destroys unrelated data. These issues are typically solved through normalization, which organizes data into a better-structured format.

**62.** (A) An attribute that is not part of any candidate key.
In normalization theory, attributes are classified based on their role in keys. A prime attribute is part of at least one candidate key. A non-prime attribute, however, is not included in any candidate key for the table. Understanding this distinction is essential for applying second and third normal form rules, which focus on functional dependencies.

**63.** (D) (I), (II), and (III)
Unnormalized databases are prone to several logical errors. Update anomalies can create conflicting data for the same entity. Insert anomalies occur when data cannot be added because a required field is unavailable. Delete anomalies happen when removing a record also deletes unrelated information. Normalization effectively addresses these issues by decomposing tables and establishing clear relationships between data items.

**64.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Third Normal Form aims to eliminate transitive dependencies, where a non-prime attribute depends on another non-prime attribute instead of directly on a key. For example, in an address table, state and city depend on the zip code, which then depends on the employee ID. Breaking these into separate tables ensures that every non-prime attribute depends only on the super key.

**65.** (C) Assertion (A) is true, but Reason (R) is false.
A clustered index determines the physical order of data in a table, and by default, the primary key serves this role. This allows for faster data retrieval based on the primary identifier. However, a table can only have one clustered index. Therefore, it is impossible for every candidate key to be organized as a clustered index simultaneously.

**66.** (A) BCNF
Boyce-Codd Normal Form is violated when a functional dependency exists where the determinant is not a super key. In the given scenario, the department attribute determines other details but is not a key itself. This stricter version of the third normal form ensures that all determinants are keys, effectively removing any remaining functional dependency issues in the table.

NODIA

**67.** (C) Organizing data to avoid logic anomalies.
Normalization is the process of structuring a relational database to reduce redundancy and improve data integrity. Its primary goal is to organize data so that each item is stored in a single logical location, thereby preventing update, insert, and delete anomalies. This creates a more stable and reliable system that is easier to maintain.

**68.** (C) 3NF - Table is in 2NF and contains multiple non-trivial multivalued dependencies.
The condition for 3NF is that the table must be in 2NF and have no transitive functional dependencies. Dealing with multiple non-trivial multivalued dependencies is actually the focus of the Fourth Normal Form. Each normal form builds upon the previous ones, adding specific rules to eliminate different types of redundancy and maintain data integrity.

totals, and managing page layouts. However, managing physical hardware aspects like disk fragmentation is a task for the operating system or specific database administration utilities, not a standard reporting tool.

**108.** (A) Storage, access, backup, and recovery.
The Oracle kernel is the core engine of the database management system. It is responsible for the fundamental operations of data storage, managing user access to records, ensuring data security, and performing critical tasks like database backup and recovery. This internal layer handles complex technical details, allowing developers and users to interact with the database using high-level commands.

**109.** (D) Defining rotation speeds of physical disks.
Scheme definition is a database administrator function that involves creating the initial structure of the database. This includes defining tables, relationships, and constraints, which are then stored in the data dictionary. While the administrator manages physical storage structures, they do not define mechanical properties of hardware, such as the rotation speeds of physical hard disks themselves.

**110.** (C) Data Pump command
The Data Pump is a high-performance utility in Oracle databases used for moving large amounts of data and metadata between systems. In Oracle 11g, it offers advanced features such as data encryption and compression, which enhance both security and efficiency during the export and import processes. This makes it a primary tool for administrators managing data migration.

**111.** (D) Hiding details to simplify interaction.
Data abstraction aims to provide users with a simplified view of the database by hiding the complex details of how data is actually stored and managed. This allows different users to interact with the data at various levels without needing to understand the underlying physical storage or complex logical structures, leading to improved usability and reduced interaction complexity.

**112.** (B) Cloud
In modern Oracle versioning, the letter 'c' stands for 'Cloud'. This designation reflects Oracle's strategic focus on integrating its database technology with cloud computing environments. Oracle 21c is designed to be a cloud-native database service, providing features that support flexible, scalable, and high-performance operations across various cloud infrastructures for businesses and developers worldwide.

**113.** (B) An attribute that is a part of the candidate key is known as a non-prime attribute.
In normalization terminology, an attribute that is a part of any candidate key is correctly called a prime attribute. A non-prime attribute is one that is not part of any candidate key. The Third Normal Form requires that a table is in 2NF and that all non-prime attributes are fully dependent only on super keys.

**114.** (C) Elimination of the Data Pump command
Oracle 11g introduced many advanced features to improve performance and manageability, including invisible indexes, virtual columns, and enhanced table partitioning. It did not eliminate the Data Pump command; on the contrary, it improved the utility by adding new options for encryption and compression. These enhancements helped administrators manage large data sets more securely and efficiently than previous versions.

**115.** (D) Atomicity
Atomicity is the transaction property that ensures a set of commands is executed as a single, indivisible unit. If any command fails, the entire transaction is aborted, and the database state is restored to its original condition. This "all or nothing" principle is difficult to maintain in traditional file systems but is a core feature of DBMS.

**116.** (C) Both (I) and (II)
For analytical purposes, data is often organized in a de-normalized format where all relevant attributes of an object are stored in the same row. This design choice optimizes read speed and simplifies data retrieval for complex reports, as all information is immediately available. Analytics typically involves historical data, which does not require strict 5NF compliance during storage.

**117.** (D) Procedural anomaly
Normalization is specifically designed to eliminate three main types of logical data

NODIA

anomalies: insert, update, and delete anomalies. These occur due to poor table structure and data redundancy. The term "procedural anomaly" is not a standard concept in normalization theory, which focuses on the structural organization of data rather than the procedural steps of code.

**118.** (B) Only (I), (II), and (III)
Oracle Forms allows for the creation of master-detail relationships to manage parent-child data links. Triggers are used to add validation checks and automate actions, such as executing code when a user clicks a button. While often used by administrators, triggers can also be defined by application developers at various levels within forms and reports to enhance functionality.

**119.** (D) It can only ever contain a single attribute without any extra attributes.
A super key is any set of attributes that uniquely identifies a row in a table. While it can consist of a single attribute, it often includes a combination of multiple attributes, including redundant ones. The minimal version of a super key, with no unnecessary attributes, is known as a candidate key. Super keys are not restricted to single attributes.

**120.** (A) A Trigger
In application development using Oracle Forms, a developer can use a trigger to execute specific logic based on user events. For instance, a validation trigger can be set to run when a user finishes entering data into a field. This allows the system to verify immediately that the input meets required criteria, such as checking age values.

**121.** (D) All of the above
A database administrator plays a central role in managing the DBMS environment. Their duties include deciding what information is stored at the logical level, understanding physical organization for performance tuning, and creating the schema definitions stored in the data dictionary. This comprehensive control ensures the system remains efficient, secure, and properly aligned with organizational data requirements.

**122.** (A) Only (I)
PL/SQL is Oracle's procedural extension to the standard SQL language. It incorporates many features of procedural programming, including variable declarations and conditional control structures like IF-THEN-ELSE. Unlike standard SQL, PL/SQL also includes the ability to handle exceptions and use various loop constructs, providing developers with a robust and flexible environment for building complex database applications and business logic.

**123.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
A table containing independent elements like lecturers and books for a single course exhibits a multivalued dependency. This situation can lead to redundant data and anomalies. Fourth Normal Form is specifically designed to address this by mandating that a table should not contain more than one such independent multivalued dependency, requiring the table to be decomposed.

**124.** (D) (I), (II), and (III)
The Oracle kernel is the foundational software component that manages the internal operations of the database system. It defines how data is stored, controls user access, and handles concurrent requests to maintain integrity. Additionally, it interprets SQL commands and provides the necessary infrastructure for database backup and recovery, ensuring that the system remains reliable and protected.

**125.** (A) Only (I), (II), (III), and (IV)
Relational database management systems are powerful because they organize data into multiple related tables using minimal assumptions. Normalization is a critical process in RDBMS design that eliminates redundancy, streamlines maintenance, and improves querying performance by ensuring each data point is stored in only one place. However, normalization is a core principle of relational databases rather than NoSQL systems.

www.nodia.in

Downloaded from www.pdf.tube

# CHAPTER 07

# Data Warehousing and Data Mining

NODIA

**May/June 2017**

**1.** Based on scope and functionality, how many types of entities are typically found in the Data Storage Layer of a data warehouse architecture?
(A) 2 types
(B) 3 types
(C) 4 types
(D) 5 types

**Oct/Nov 2006**

**2.** How do real-time analytics conceptually improve marketing campaigns using a data warehouse?
(A) By creating standalone databases that isolate customer service metrics from sales
(B) By strictly preventing internal operational data from mixing with external market data
(C) By providing a unified 360-degree customer view for sentiment and personalization
(D) By utilizing virtual point-to-point networks to directly query unstructured social media traffic

**May/June 2005**

**3.** What is the precise definition of "metadata" in a data warehouse environment?
(A) Structured analytical models used for long-term forecasting
(B) Raw, unprocessed transaction records from operational systems
(C) Information describing data stored within the warehouse system
(D) Final graphical reports presented directly to executive users

**Oct/Nov 2021**

**4.** Which statement correctly reflects the management of data warehouses?
(A) Data warehouse projects are best viewed as simple stopgap measures that require minimal maintenance
(B) A data warehouse is only considered a good investment if it replaces the operational systems entirely
(C) Management must recognize that maintenance of the data warehouse structure is as critical as any other mission-critical application
(D) Embarking on a data warehousing program significantly reduces the demand on operational systems for better data

**May/June 2010**

**5.** How do data lakes conceptually differ from data warehouses?
(A) Data lakes store only structured data, while data warehouses store unstructured data
(B) Data lakes store data in raw form, while data warehouses store data in a highly structured and transformed form
(C) Data lakes are designed exclusively for departmental analysis, while data warehouses are used for raw operational processing
(D) Data lakes do not support big data, while data warehouses are built exclusively for big data

**Oct/Nov 2022**

**6.** Which statement correctly describes the "Association" approach in data mining?
(A) It recognizes patterns that describe the group to which an item belongs based on past classified examples
(B) It links occurrences within a single event, such as items purchased during one visit
(C) It groups data into segments depending on common features without prior classification
(D) It builds models to determine the relationship between variables to predict bankruptcy

**May/June 2014**

**7.** Data locked up in a myriad of computer systems that is exceedingly difficult to access for executives and decision-makers is best defined by which of the following terms?
(A) Data lake

Oct/Nov 2017

**24.** Which statement correctly characterizes Central Data Warehouses?
(A) They are distributed across multiple physical databases using localized LANs
(B) They are virtual point-to-point systems that avoid storing redundant data
(C) They serve exclusively as staging areas for unstructured data lakes
(D) They are single databases using advanced RDBMS for specific functional areas

May/June 2009

**25.** Which conceptual distinction accurately separates OLAP from OLTP?
(A) OLAP processes transactions online, whereas OLTP provides summarized multidimensional views
(B) OLAP analyzes historical data for decisions, while OLTP processes current transactions online
(C) OLAP contains current data, whereas OLTP transforms historical data into strategic information
(D) OLAP is used exclusively for operational databases, whereas OLTP is used for data mining

Oct/Nov 2023

**26.** How is a "Virtual Data Warehouse" defined in terms of its operational strategy?
(A) A single physical repository containing all historical enterprise data
(B) A distributed cloud environment for managing unstructured big data
(C) A departmental database strictly limited to localized subject data
(D) A strategy enabling direct user access to operational data via a network

May/June 2022

**27.** Which statement correctly describes the effectiveness of Business Intelligence (BI)?
(A) BI is most effective when it combines data derived from the market (external data) with data from company sources (internal data)
(B) BI is most effective when it relies entirely on internal operational data
(C) BI tools empower organizations by strictly isolating external market analysis from internal financial records
(D) BI applications operate exclusively within the Data Extraction Layer of the architecture

Oct/Nov 2012

**28.** A rule-based system used in software development to provide answers in place of a human expert relies on what specific type of statements?
(A) If-then statements
(B) While-do statements
(C) For-next statements
(D) Switch-case statements

May/June 2015

**29.** Which statement correctly describes the nature of operational systems in an enterprise?
(A) They are informational knowledge-based systems used for multi-dimensional analysis
(B) They are exclusively focused on long-term historical trends spanning multiple areas
(C) They are the computerized backbone systems performing day-to-day enterprise tasks
(D) They store data in raw form without any structured transformation

Oct/Nov 2019

**30.** In order to achieve the "Integrated" characteristic in a data warehouse, which conceptual process must occur?
(A) The data must be isolated into distinct data marts to prevent overlap
(B) The data must be kept in its raw format to maintain operational fidelity
(C) The database must be fully normalized to eliminate all historical reports
(D) Inconsistencies like naming and encoding must be unified across source systems

May/June 2019

**31.** Which statement regarding the strategy of building a copy of operational data is incorrect?
(A) It involves building a copy of the operational data from a single operational system
(B) It has the advantage of being both simple and fast
(C) It guarantees high-quality data outputs even if the existing operational data is of poor quality
(D) If access to the data has not been thought through, it can create significant problems

Click Here to Buy book on Amazon

Oct/Nov 2018

**16.** Which of the following best defines "data granularity" in the context of a data warehouse?
(A) The level of details considered in a model or decision-making process
(B) The physical separation of data across different databases
(C) The aggregation of data from multiple operational systems
(D) The historical timeframe represented by the data stored

May/June 2024

**17.** Which statement is correct regarding the design of data warehouses?
(A) Designing a data warehouse is quite close to Business Process Reengineering (BPR)
(B) The ideal design strategy for a data warehouse is top-down rather than outside-in
(C) Data warehouse users typically know exactly as much about their wants and needs as operational users
(D) Robust working prototypes are rarely essential because requirements are easily defined

Oct/Nov 2013

**18.** The end-users of a data warehouse are generally categorized into how many broad categories?
(A) 2 broad categories
(B) 3 broad categories
(C) 4 broad categories
(D) 5 broad categories

May/June 2011

**19.** What is the fundamental mechanism behind "In-memory technologies" in data warehousing?
(A) Processing large data sets exclusively on decentralized magnetic hard drives to save costs
(B) Utilizing ledger-based blockchain systems to record transaction logs permanently
(C) Distributing data processing tasks to edge devices like mobile phones
(D) Processing data in system RAM to accelerate analytics and actionable reporting

Oct/Nov 2020

**20.** The "Non-volatile" nature of a data warehouse means that the data is read-only. Under what conceptual condition can this data be updated or deleted?
(A) When there is a regulatory or statutory obligation to do so
(B) When an end-user requests a modification to their historical purchasing patterns
(C) When the operational system undergoes a routine nightly batch update
(D) When the ETL job detects a minor inconsistency in naming conventions

May/June 2013

**21.** Which statement correctly portrays Distributed Data Warehouses?
(A) They typically involve the least amount of redundant data and the simplest updating processes
(B) They consist of a single centralized repository connecting all end-users to one physical database
(C) They utilize components across multiple databases, often increasing redundancy and complexity
(D) They allow end-users to directly query operational systems without loading or maintaining redundant data

NODIA

Oct/Nov 2015

**22.** A data warehouse primarily stores historical data. Up to what long time horizon does data warehouse data typically represent?
(A) Up to 3 years
(B) Up to 5 years
(C) Up to 10 years
(D) Up to 15 years

May/June 2020

**23.** Which of the following represents the core conceptual difference between Operational Systems and Informational Systems?
(A) Operational systems manage historical data up to 10 years, whereas informational systems manage current transactional data
(B) Operational systems allow only read-only access, whereas informational systems allow frequent updates and deletions
(C) Operational systems use multi-dimensional analytical models, whereas informational systems rely on basic relational models
(D) Operational systems focus on a single area for day-to-day operations, whereas informational systems span multiple areas for planning and forecasting

navigational paths
(D) To deliver the final tabular and graphical reports directly to the end-user

**Oct/Nov 2014**

**58.** Which statement about emerging trends in data warehousing is incorrect?
(A) In-database analytics require significant data movement back and forth to other systems for analysis
(B) Physical and logical consolidation is achieved through virtualization, compression, and multi-tenant databases
(C) In-memory technologies bring car-like performance by processing large data sets in system RAM
(D) Use of commodity servers helps reduce vendor lock-in and long-term costs

**May/June 2019**

**59.** Which description best represents the overall framework of data warehousing?
(A) A decentralized set of temporary operational applications for clerical staff
(B) A system used exclusively for day-to-day order entry processing
(C) An enterprise-wide framework for managing informational data within the organization
(D) A standalone graphical reporting tool detached from historical data

**Oct/Nov 2006**

**60.** Based on scope and functionality, the Data Storage Layer contains three types of entities. Which of the following is NOT one of these entities?
(A) Data Warehouse
(B) Ledger Base Store (LBS)
(C) Data Mart
(D) Operational Data Store (ODS)

**May/June 2021**

**61.** Match the Data Mining Approaches in List I with their examples/descriptions in List II.
List I: (Mining Approaches)
P. Associations
Q. Classifications
R. Clustering
S. Forecasting
List II: (Descriptions)
1. Evaluating a credit card proposal based on past classified examples
2. Discovering population segments depending on buying habits from unclassified data
3. Linking the number of items purchased by a customer in a single visit
4. Predicting bankruptcy using a set of ratios and financial variables
(A) P-1, Q-3, R-4, S-2
(B) P-4, Q-2, R-1, S-3
(C) P-3, Q-1, R-2, S-4
(D) P-4, Q-2, R-3, S-1

**Oct/Nov 2010**

**62.** Consider the following statements regarding data warehouse design:
I Designing a data warehouse is viewed as quite close to Business Process Reengineering (BPR).
II The ideal design strategy for a data warehouse is consistently top-down as opposed to outside-in.
Which of the above statements is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**May/June 2005**

**63.** Match the Data Warehouse Architecture Layers in List I with their functions in List II.
List I: (Architecture Layers)
P. Data Source Layer
Q. Staging Area
R. Data Logic Layer
S. Metadata Layer
List II: (Functions)
1. Stores business rules that affect what reports look like
2. Holds information about the data stored in the warehouse
3. Feeds data from operations, web logs, and third-party databases
4. Area where data sits prior to being scrubbed and transformed
(A) P-3, Q-4, R-1, S-2
(B) P-2, Q-4, R-1, S-3
(C) P-4, Q-1, R-3, S-2
(D) P-3, Q-1, R-4, S-2

**Oct/Nov 2022**

**64.** Consider the following statements regarding the advantages provided by OLAP applications:

Downloaded from www.pdf.tube

Oct/Nov 2005

**32.** Which of the following is NOT one of these major approaches?
(A) Associations
(B) Compilations
(C) Classifications
(D) Clusters

May/June 2012

**33.** Which statement regarding the layers in a Data Warehouse architecture is incorrect?
(A) In the Data Extraction Layer, minimal data cleansing occurs, but major transformation is unlikely
(B) The ETL Layer is exclusively used for storing tabular and graphical reports for end-users
(C) The Staging Area is where data sits prior to being scrubbed and transformed
(D) The ETL design phase is often the most time-consuming phase in a data warehousing project

Oct/Nov 2009

**34.** What serves as the primary inspiration for the structure of Artificial Neural Networks (ANNs)?
(A) The physical architecture of modern integrated circuits
(B) The operational data structure of relational databases
(C) The hierarchical structure of organizational management
(D) The biological information processing model of the interconnected human brain

May/June 2018

**35.** In a general data warehouse architecture, all of the following are distinct layers, EXCEPT:
(A) Data Divestment Layer
(B) Staging Area
(C) Data Logic Layer
(D) Metadata Layer

Oct/Nov 2016

**36.** What is the key benefit of physical and logical consolidation in burgeoning data warehouses?
(A) Reducing costs via virtualization and multi-tenancy instead of linear hardware scaling
(B) Allowing organizations to physically store data on single uncompressed hard drives
(C) Eliminating the need for any form of data transformation or cleansing
(D) Converting all multi-dimensional OLAP cubes into basic flat files for faster access

May/June 2016

**37.** Which of the following statements about data storage formats is incorrect?
(A) Data lakes store highly structured data exclusively, whereas data warehouses manage only raw data
(B) Data lakes store data in raw form
(C) Data warehouses store data in a highly structured and transformed form
(D) Big data is stored in both structured and unstructured forms

Oct/Nov 2010

**38.** Data warehouse end-users are broadly categorized into three groups. Which of the following is NOT one of these standard categories?
(A) Executives and managers
(B) Power users (business and financial analysts, engineers, etc.)
(C) Support users (clerical, administrative, etc.)
(D) System architects (database administrators, network engineers)

NODIA

May/June 2021

**39.** What is the primary intention of storing Time-variant data in a data warehouse?
(A) To facilitate immediate operational updates and deletions
(B) To primarily support daily order entry and payroll functions
(C) To ensure the database maintains absolute data granularity in real-time
(D) To provide a long time horizon intended for data mining and forecasting

Oct/Nov 2008

**40.** Which statement regarding data mining approaches is incorrect?
(A) Classification recognizes patterns describing the group to which an item belongs using classified past data
(B) Clustering discovers different groupings depending on common features in unclassified past examples
(C) Forecasting builds models to determine relationships between variables to predict future behavior
(D) Association specifically builds statistical models to classify risk based exclusively on predefined segments

(B) Data in jail
(C) Information silo
(D) Virtual data

**Oct/Nov 2014**

**8.** What is the conceptual function of the Data Logic Layer within the data warehouse architecture?
(A) It applies transformations to raw data directly extracted from operational sources
(B) It stores business rules that govern the presentation and appearance of reports
(C) It serves as the physical storage location for the data mart and ODS
(D) It manages the ETL job status and user access history

**May/June 2023**

**9.** Which of the following correctly identifies the information managed by the System Operations Layer?
(A) The logical data model and data dictionary
(B) Operational logs including ETL status, system performance, and access history
(C) The rules to map, translate, and transform data sources to warehouse elements
(D) Tabular and graphical reports that reach the end-users

**Oct/Nov 2011**

**10.** Oracle's Hybrid Columnar Compression is an advanced method designed to match organization data growing at what rate, allowing valuable data storage without proportional cost increases?
(A) 5X
(B) 10X
(C) 50X
(D) 100X

**May/June 2008**

**11.** Which statement is correct regarding "Engineered systems" in data warehousing?
(A) They are decentralized systems running strictly on mobile edge devices
(B) They are virtual data environments that rely completely on commodity servers to reduce lock-in
(C) They are operational transactional databases that process current data online
(D) They are preconfigured hardware optimized for specific workloads to ensure performance

**Oct/Nov 2024**

**12.** Which of the following defines "Machine Learning" accurately?
(A) A rule-based system using specific if-then logic to deduce factual data
(B) A logic engine designed to solve complex tasks via conventional code
(C) A system using historical data to find patterns without explicit rules
(D) A centralized repository that records non-volatile operational transactions

**May/June 2025**

**13.** Conceptually, how does "Clustering" differ from "Classification" in data mining?
(A) Clustering groups unclassified data, while Classification learns from pre-grouped examples
(B) Classification discovers groupings based on attributes, while Clustering uses pre-grouped data
(C) Clustering predicts future behavior, whereas Classification associates events in a single visit
(D) Classification relies on sequence mapping, whereas Clustering is used for targeted promotions

**Oct/Nov 2025**

**14.** What does the "Subject-oriented" characteristic of a data warehouse fundamentally imply?
(A) The data is normalized to achieve the highest level of transactional efficiency
(B) The data reflects the current operational values of the enterprise
(C) The data focuses on business subjects by gathering only specific objects for analysis
(D) The data represents a singular functional area exclusively, such as a localized payroll system

**May/June 2007**

**15.** Which statement correctly identifies a subsystem of an Expert System and its function?
(A) The Extraction Engine extracts logic from operational databases
(B) The Staging Engine scrubs the data before applying knowledge rules
(C) The Data Dictionary stores the tabular reports generated by the user interface
(D) The Inference Engine applies rules to facts to deduce new facts via reasoning

Click Here to Buy book on Amazon

May/June 2022

**49.** Which of the following is NOT recognized as an emerging trend in data warehousing and analytics?
(A) Migration of all data entirely to paper-based offline ledgers to enhance security
(B) Engineered systems becoming a preferred approach for large scale information management
(C) In-database analytics simplifying analysis
(D) AI Operations, Cloud & Automation becoming a must

Oct/Nov 2023

**50.** When an enterprise is considering data warehouse options regarding data redundancy, it typically evaluates three levels. Which of the following is NOT one of these three levels?
(A) Virtual or Point-to-Point Data Warehouses
(B) Central Data Warehouses
(C) Decentralized Edge Warehouses
(D) Distributed Data Warehouses

May/June 2016

**51.** Why are AI Operations and Cloud integration anticipated to become a must in the future of data warehousing?
(A) Because they will replace all need for operational transaction processing systems entirely
(B) Because artificial intelligence is required to read uncompressed XML flat files
(C) Because legacy mainframes can no longer support standalone databases
(D) Because ML algorithms generate proactive insights that improve operational efficiency

Oct/Nov 2009

**52.** Which statement regarding the Virtual Data Warehouse strategy is incorrect?
(A) It allows end-users to get at operational databases directly using tools
(B) It provides flexibility and a minimum amount of redundant data to be maintained
(C) It often provides a starting point for organizations to learn what end-users are looking for
(D) It eliminates all unplanned query loads on operational systems entirely

May/June 2023

**53.** All of the following are considered typical day-to-day operational backbone systems of an enterprise, EXCEPT:
(A) Order entry system
(B) Inventory system
(C) Marketing planning system
(D) Payroll system

Oct/Nov 2018

**54.** What is the ultimate optimal strategy for developing a data warehouse?
(A) Copying the entire operational system structure into a secondary hard drive
(B) Designing a centralized system top-down without end-user input to ensure consistency
(C) Building populated prototype warehouses based on analyzed user population needs
(D) Implementing a strictly virtual point-to-point network permanently to avoid any redundant data

May/June 2007

**55.** An Expert System is divided into specific subsystems. Which of the following is NOT identified as one of the fundamental parts or subsystems of an Expert System?
(A) Transformation Engine
(B) Inference Engine
(C) Knowledge Base
(D) User Interface

Oct/Nov 2025

**56.** Which of the following statements regarding the Metadata Layer is incorrect?
(A) It houses the operational transaction processing engine for day-to-day operations
(B) It is where information about the data stored in the data warehouse system is stored
(C) It contains the navigational paths and rules for browsing in the data warehouse
(D) A logical data model would be an example of something found in this layer

May/June 2012

**57.** What is the main purpose of utilizing a Staging Area in the data warehouse architecture?
(A) To provide a common area for data to reside before scrubbing and transformation
(B) To apply complex business logic that dictates what the final report looks like
(C) To store metadata components including

Downloaded from www.pdf.tube

May/June 2006

**41.** Arrange the following steps involved in establishing a virtual data warehouse environment in the correct chronological order:
I Monitoring how the data warehouse facilities are actually used.
II Installing a set of data access, data directory, and process management facilities.
III Based on actual usage, creating a physical data warehouse to support high-frequency requests.
IV Training the end-users.
(A) (II), (IV), (I), (III)
(B) (I), (II), (IV), (III)
(C) (IV), (II), (III), (I)
(D) (II), (I), (IV), (III)

Oct/Nov 2007

**42.** Which of the following statements regarding data warehouse scope is incorrect?
(A) A data warehouse is generally used on an enterprise level
(B) A data mart only contains required subject-specific data for local analysis
(C) Data marts operate enterprise-wide, whereas data warehouses focus on departments
(D) The broader the scope, the more value the data warehouse is to the enterprise

May/June 2008

**43.** Artificial Neural Networks have a multitude of real-world applications in the business domain. Which of the following is NOT explicitly classified as an application of ANN?
(A) Signature and bank note verification
(B) Setting daily operational naming conventions
(C) Mortgage underwriting
(D) Identifying tax fraud

Oct/Nov 2013

**44.** Which of the following is NOT typically considered a valid data source for the Data Source Layer in a data warehouse?
(A) Web server logs providing user browsing data
(B) Internal market research data
(C) Third-party data such as census and demographics
(D) Future unrecorded operational projections generated without historical data

May/June 2015

**45.** What is the primary role of the Data Presentation Layer in a data warehouse?
(A) It performs intense data cleansing and intelligence application
(B) It stores the historical, non-volatile raw data for long-term archiving
(C) It delivers information to users via tabular reports, graphical charts, or alerts
(D) It actively captures daily transactional operational data from point-of-sale systems

Oct/Nov 2012

**46.** Which of the following statements regarding the "Subject-oriented" characteristic of a data warehouse is incorrect?
(A) Data revolves around the enterprise's subjects rather than individual applications
(B) Database normalization is identical to subject orientation
(C) Subject orientation can be extremely beneficial in decision-making
(D) It refers to the process of gathering only the necessary objects

May/June 2011

**47.** When is Business Intelligence (BI) considered to be most effective?
(A) When it relies exclusively on external data sources such as third-party surveys
(B) When it integrates external market data with internal sources for a complete view
(C) When it focuses solely on product pricing and ignores strategic broad-level directions
(D) When it utilizes only flat files and restricts query capabilities

Oct/Nov 2020

**48.** Which statement about designing data warehouses is incorrect?
(A) It often involves thinking in terms of broader and more difficult to define business concepts
(B) End-users typically know exactly what they need as a bare minimum before design begins
(C) Designing a data warehouse is very different from designing traditional operational systems
(D) Robust working prototypes are essential to help users visualize their requirements

NODIA

I They enable managers to model problems that would be impossible using less flexible systems.
II They increase productivity and make business users more self-sufficient without depending on IT for scheme changes.
III They replace the need for traditional data warehousing by operating entirely on real-time operational transactions.

Which of the above statements is/are correct?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) All (I), (II), and (III)

**May/June 2018**

**65.** Identify the correct pair matching a data architecture layer to its corresponding tool or function.
(A) Metadata Layer - Stores rules to map, translate, and transform data sources
(B) ETL Layer - Tabular and graphical reports sent via email
(C) Data Presentation Layer - Extracts raw data from web server logs
(D) System Operations Layer - Stores business logic affecting report appearance

**Oct/Nov 2016**

**66.** Business Intelligence (BI) includes several types of applications and technologies. Consider the following:
I Decision Support Systems (DSS)
II Online Analytical Processing (OLAP)
III Data Mining
IV Automated Teller Machine (ATM) Switching Systems

Which of the above are recognized BI applications?
(A) Only (I), (II), and (III)
(B) Only (I), (II), and (IV)
(C) Only (II), (III), and (IV)
(D) All (I), (II), (III), and (IV)

**May/June 2014**

**67.** Arrange the following layers of a data warehouse architecture in the typical sequential flow of data from extraction to processing:
I Data Logic Layer
II Data Extraction Layer
III Data Presentation Layer
IV ETL Layer
(A) (II), (IV), (I), (III)
(B) (IV), (II), (III), (I)
(C) (II), (I), (IV), (III)
(D) (IV), (I), (II), (III)

**Oct/Nov 2007**

**68.** Consider the following statements regarding organizational data systems:
I The phenomenon described as "data in jail" refers to billions of bytes of operational data that are locked up and exceedingly difficult for executives to access.
II Operational systems are completely isolated from the enterprise and are never rewritten, enhanced, or maintained over the years.

Which of the above statements is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**May/June 2025**

**69.** Consider the following statements regarding the metadata component of a data warehouse:
I It contains the description of the data warehouse and the data dictionary.
II It provides rules to map, translate, and transform data sources to warehouse elements.
III It functions as the primary graphical interface for the end-user's daily OLTP tasks.

Which of the above statements is/are correct?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) All (I), (II), and (III)

**Oct/Nov 2019**

**70.** Match the Database types in List I with their examples in List II.
List I: (Database/Method)
P. NoSQL Database
Q. Ledger based DBMS
R. Engineered System
S. Data compression method
List II: (Examples)
1. Hybrid Columnar Compression
2. Amazon QLDB or Blockchain-based
3. Mongo DB and Redis
4. Integrated database appliances
(A) P-1, Q-4, R-2, S-3

Click Here to Buy book on Amazon

May/June 2006

**83.** Match the ANN Applications in List I with their respective domains in List II.

List I: (ANN Application)

P. Accounting domain
Q. Finance domain
R. Marketing domain
S. Human resources domain

List II: (Domains)

1. Classification of consumer spending patterns
2. Determining personnel resource requirements
3. Identifying tax fraud
4. Mortgage underwriting

(A) P-1, Q-2, R-3, S-4
(B) P-4, Q-3, R-2, S-1
(C) P-4, Q-3, R-2, S-1
(D) P-3, Q-4, R-1, S-2

Oct/Nov 2017

**84.** Consider the following statements describing the strategy of building a copy of operational data into a data warehouse:

I It has the advantage of being both simple and fast.
II It completely eliminates the need for any ETL tool or data storage layer.
III It can create significant problems if the existing data is of poor quality or access has not been well thought through.

Which of the above statements is/are correct?

(A) Only (I) and (II)
(B) Only (I) and (III)
(C) Only (II) and (III)
(D) All (I), (II), and (III)

May/June 2008

**85.** Consider the following statements regarding the layers of a Data Warehouse:

I The Staging Area is where data sits prior to being scrubbed and transformed.
II The ETL Layer is where data cleansing happens and logic is applied to transform data from a transactional nature to an analytical nature.

Which of the above statements is/are correct?

(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

NODIA

Oct/Nov 2013

**86.** Match the Data Redundancy Options in List I with their descriptions in List II.

List I: (Redundancy Options)

P. Virtual Data Warehouse
Q. Central Data Warehouse
R. Distributed Data Warehouse
S. Data Mart

List II: (Descriptions)

1. Used on a business division/department level containing subject-specific data
2. Single physical database containing data for a specific functional area built around advanced RDBMS
3. Components are spread across different physical databases involving complex loading processes
4. End-users get at operational databases directly using data access network tools

(A) P-1, Q-2, R-3, S-4
(B) P-4, Q-2, R-3, S-1
(C) P-1, Q-4, R-2, S-3
(D) P-3, Q-1, R-4, S-2

May/June 2015

**87.** The Data Source Layer receives data from various feeds to supply the data warehouse. Consider the following sources:

I HR and marketing systems data
II Web server browsing logs
III Internal market research data
IV Third-party demographic census data

Which of the above represent valid sources for this layer?

(A) Only (I), (II), and (III)
(B) Only (I), (III), and (IV)
(C) Only (II), (III), and (IV)
(D) All (I), (II), (III), and (IV)

Oct/Nov 2012

**88.** Match the BI Business Decisions in List I with their scope/examples in List II.

List I: (Business Decisions)

P. Basic operating decisions
Q. Strategic business decisions
R. External data
S. Internal data

List II: (Scope)

1. Priorities, goals, and directions at the broadest level
2. Derived from the market in which a company operates

(B) P-4, Q-1, R-3, S-2
(C) P-1, Q-3, R-2, S-4
(D) P-2, Q-4, R-1, S-3

**May/June 2020**

**77.** Consider the following statements regarding the recognized components of an Expert System:
I User Interface
II Knowledge Base
III Inference Engine
Which of the above statements is/are correct?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) All (I), (II), and (III)

**Oct/Nov 2015**

**78.** Match the Emerging Trends in List I with their corresponding technologies/concepts in List II.
List I: (Emerging Trends)
P. Physical and logical consolidation
Q. Real-time analytics
R. Engineered systems
S. In-memory technologies
List II: (Technologies)
1. System RAM processing for high-speed performance
2. Preconfigured hardware appliances optimized for specific workloads
3. Virtualization, compression, and multi-tenant databases
4. 360-degree view of customer base for sentiment analysis
(A) P-2, Q-3, R-4, S-1
(B) P-1, Q-2, R-3, S-4
(C) P-4, Q-1, R-3, S-2
(D) P-3, Q-4, R-2, S-1

**May/June 2013**

**79.** Consider the following statements regarding Artificial Intelligence concepts:
I Machine Learning (ML) is a field concerned with emulating human thoughts by requiring strict, explicit procedural rules to find patterns.
II An Expert System utilizes a Knowledge Base and an Inference Engine to solve complex problems through reasoning, mainly represented as if-then rules.
Which of the above statements is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**Oct/Nov 2021**

**80.** Identify the INCORRECT pair matching an emerging trend to its enabling technology.
(A) Autonomous/self-healing DB - Automates many backend tasks
(B) Time series DB - Designed specifically for analytics/event trails
(C) Ledger based DBMS - Inspired by the blockchain
(D) Edge use cases DBMS - Requires massive centralized commodity server clusters

**May/June 2024**

**81.** Artificial Neural Networks (ANN) have numerous real-world applications. Consider the following domains:
I Mortgage underwriting
II Foreign exchange rate forecasting
III Classification of consumer spending patterns
IV Determining personnel resource requirements
Which of the above represent ANN applications?
(A) Only (I), (II), and (III)
(B) Only (I), (III), and (IV)
(C) Only (II), (III), and (IV)
(D) All (I), (II), (III), and (IV)

**Oct/Nov 2008**

**82.** Match the Expert System components in List I with their correct definitions in List II.
List I: (Components)
P. Inference Engine
Q. Knowledge Base
R. User Interface
S. Rule-based system
List II: (Definitions)
1. A collection of facts and rules
2. Allows a non-expert user to query and receive advice
3. Uses a set of if-then statements to act upon assertions
4. Applies rules to known facts to deduce new facts
(A) P-4, Q-1, R-2, S-3
(B) P-1, Q-4, R-3, S-2
(C) P-3, Q-2, R-1, S-4
(D) P-2, Q-3, R-4, S-1

Downloaded from www.pdf.tube

(C) Forecasting
(D) Sequencing

Oct/Nov 2016

**108.** Given below are two statements: one is labelled as Assertion (A) and the other is labelled as Reason (R).
Assertion (A): The data contained within a Data Warehouse is considered non-volatile.
Reason (R): Data Warehouse data is read-only, meaning it cannot be updated, created, or deleted unless there is a regulatory or statutory obligation to do so.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2014

**109.** To maintain security and monitor system performance, an IT auditing team requires a log of ETL job status and user access history within a new data warehouse environment. Which layer provides this capability?
(A) Data Presentation Layer
(B) Data Source Layer
(C) Metadata Layer
(D) System Operations Layer

Oct/Nov 2007

**110.** Given below are two statements: one is labelled as Assertion (A) and the other is labelled as Reason (R).
Assertion (A): Burgeoning data warehouses must be physically and logically consolidated to help reduce costs.
Reason (R): Translating ten times the data into ten times the cost is not a sustainable financial strategy for managing expanding information.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

NODIA

May/June 2025

**111.** Following the implementation of a new analytical system, retail managers are no longer dependent on IT to make scheme changes; they can model previously impossible problems and maintain high self-sufficiency. What characteristic of successful OLAP applications does this highlight?
(A) The inherent inflexibility of system operations logs
(B) The restriction of end-users to support roles only
(C) The elimination of all metadata from the database
(D) The increased productivity of business managers

Oct/Nov 2019

**112.** Given below are two statements: one is labelled as Assertion (A) and the other is labelled as Reason (R).
Assertion (A): The data warehouse remains relevant despite the advent of data lakes.
Reason (R): Data lakes store large scale data in raw form, whereas data warehouses store data in a highly structured and transformed form.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2009

**113.** Given below are two statements: one is labelled as Assertion (A) and the other is labelled as Reason (R).
Assertion (A): Designing data warehouses is very different from designing traditional operational systems.
Reason (R): Data warehouse users typically know exactly as much about their wants and needs as operational users.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.

3. Product positioning or pricing
4. Financial and operations data

(A) P-1, Q-3, R-4, S-2
(B) P-3, Q-1, R-2, S-4
(C) P-4, Q-2, R-1, S-3
(D) P-2, Q-4, R-3, S-1

**May/June 2011**

**89.** Consider the following statements about Informational Systems:

I They analyze data and support in taking major decisions like how the enterprise will operate in the future.
II They normally focus upon a single operational area strictly.
III They often span a number of different areas and require large amounts of related operational data.

Which of the above statements is/are correct?

(A) Only (I) and (II)
(B) Only (I) and (III)
(C) Only (II) and (III)
(D) All (I), (II), and (III)

**Oct/Nov 2020**

**90.** Identify the INCORRECT pair matching a Data Mining approach to its definition.

(A) Classifications - Predicting bankruptcy using unclassified demographic data
(B) Associations - Linking events over a period of time in a single event
(C) Clustering - Discovering groupings within data depending on common features
(D) Forecasting - Determining the relationship between parameters to predict future behavior

**May/June 2022**

**91.** Given below are two statements: one is labelled as Assertion (A) and the other is labelled as Reason (R).

Assertion (A): Database normalization is identical to the concept of subject orientation in a data warehouse.

Reason (R): Subject orientation refers to the process of gathering only the necessary objects beneficial in decision-making.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2023**

**92.** A bank's business users want final analytical reports to format negative balances in red text. The IT team configures these formatting rules in a specific layer that affects what the report looks like, without altering underlying data transformation rules. Which layer stores these rules?

(A) Data Extraction Layer
(B) Data Storage Layer
(C) Data Logic Layer
(D) Metadata Layer

**May/June 2016**

**93.** Developing and managing data warehouses requires specific strategic approaches. Consider the following:

I The ultimate optimal strategy analyzes user population issues, questions, and needs to build prototype warehouses.
II Developing a data warehouse is an evolutionary approach.
III The ideal design strategy is often outside-in as opposed to top-down.
IV Data warehouse projects require careful marketing and management to be successful.
V Implementing a data warehouse creates demands upon operational systems for better, consistent data.

(A) Only (I), (II), (III), and (IV)
(B) Only (II), (III), (IV), and (V)
(C) Only (I), (III), (IV), and (V)
(D) All (I), (II), (III), (IV), and (V)

**Oct/Nov 2009**

**94.** A risk management team has thousands of past credit evaluations that are already categorized as "High Risk" or "Low Risk". They want to use these categorized examples to evaluate new insurance proposals. Which data mining activity applies here?

(A) Clustering
(B) Association
(C) Classification
(D) Virtualization

Click Here to Buy book on Amazon

(B) P-2, Q-3, R-1, S-4
(C) P-3, Q-2, R-4, S-1
(D) P-4, Q-1, R-3, S-2

**May/June 2009**

**71.** The emerging trends in data warehousing reflect new operational requirements. Consider the following:
I Enterprises requiring more capable data warehouses to handle IoT and social media traffic.
II Physical and logical consolidation using multi-tenant databases to reduce costs.
III In-database analytics simplifying analysis with native SQL and R integration.
IV Shifting entirely away from data storage towards fully volatile memory caches without backend databases.
Which of the above represent recognized trends?
(A) Only (I), (II), and (III)
(B) Only (I), (III), and (IV)
(C) Only (II), (III), and (IV)
(D) All (I), (II), (III), and (IV)

**Oct/Nov 2011**

**72.** Match the Type of End-user in List I with their examples in List II.
List I: (End-user Type)
P. "Power" users
Q. Support users
R. Executives
S. Operational users
List II: (Examples)
1. Run day-to-day transaction backbone systems
2. Business and financial analysts, engineers
3. Make strategic decisions and broader operational directions
4. Clerical and administrative staff
(A) P-4, Q-3, R-2, S-1
(B) P-2, Q-4, R-3, S-1
(C) P-3, Q-1, R-4, S-2
(D) P-1, Q-2, R-3, S-4

**May/June 2010**

**73.** Consider the following statements regarding data redundancy options:
I A Central Data Warehouse typically contains data from a single operational system and relies exclusively on manual flat files.
II Distributed Data Warehouses push decision-making down to lower levels and usually involve the most redundant data and complex updating processes.
Which of the above statements is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**Oct/Nov 2024**

**74.** Identify the correct pair distinguishing OLAP from OLTP.
(A) OLAP - Contains current transactional data
(B) OLTP - Enables calculation engine for variances and ratios
(C) OLAP - Designed for live ad hoc data access and historical decision-making
(D) OLTP - Performs strategic multi-dimensional data mining

**May/June 2017**

**75.** Data Warehouse fundamentally differs from operational systems based on key characteristics. Consider the following:
I Subject-oriented
II Integrated
III Time-variant
IV Non-volatile
Which of the above represent these essential characteristics?
(A) Only (I), (II), and (III)
(B) Only (I), (III), and (IV)
(C) Only (II), (III), and (IV)
(D) All (I), (II), (III), and (IV)

**Oct/Nov 2005**

**76.** Match the Essential Characteristics of a Data Warehouse in List I with their appropriate descriptions in List II.
List I: (Essential Characteristics)
P. Subject-oriented
Q. Integrated
R. Time-variant
S. Non-volatile
List II: (Descriptions)
1. Data represents a long time horizon, up to 10 years
2. Gathers only the necessary objects beneficial for decision-making
3. Data is read-only and cannot be updated
4. Inconsistencies like naming conventions are eliminated
(A) P-3, Q-2, R-4, S-1

NODIA

(B) Classification
(C) Clustering
(D) Point-in-time Forecasting

**Oct/Nov 2006**

**102.** Emerging trends are shaping the future of Data Warehousing and Analytics. Consider the following:
I Using real-time analytics for comprehensive 360-degree customer sentiment analysis.
II Engineered systems preconfigured for specific workloads to deliver the highest performance.
III Data compression methods like Hybrid Columnar Compression enabling higher-volume analytics without significant cost increases.
IV In-memory technologies processing data sets in system RAM.
V AI Operations and Cloud generating actionable insights to make operations efficient.
Which of the above represent recognized trends?
(A) Only (I), (II), (III), and (IV)
(B) Only (I), (II), (IV), and (V)
(C) Only (II), (III), (IV), and (V)
(D) All (I), (II), (III), (IV), and (V)

**May/June 2021**

**103.** Before a bank applies complex transformations and analytical logic to incoming raw credit card transaction data, they route the data to a common interim storage location to make subsequent processing easier. Which architectural layer are they utilizing?
(A) Data Presentation Layer
(B) Staging Area
(C) Metadata Layer
(D) System Operations Layer

**Oct/Nov 2010**

**104.** Given below are two statements: one is labelled as Assertion (A) and the other is labelled as Reason (R).
Assertion (A): In data mining, the clustering algorithm assumes that past examples are already classified into groups.
Reason (R): Clustering discovers different groupings within the data depending on common features or attributes from unclassified demographic data.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2005**

**105.** A retail chain's finance department builds statistical models using historical ratios and financial variables to predict the future likelihood of bankruptcy among their regional suppliers. Which data mining approach does this represent?
(A) Classification
(B) Association
(C) Forecasting
(D) Clustering

**Oct/Nov 2022**

**106.** Consider the following statements regarding data redundancy options in data warehouses:
I Virtual Data Warehouses minimize redundant data but put a large query load on operational systems.
II Central Data Warehouses are a single physical database containing data for a specific functional area.
III Distributed Data Warehouses push decision-making down to LANs or local computers.
IV Distributed Data Warehouses usually involve the most complex loading and updating processes.
V Point-to-Point Data Warehouses centralize all external data into a non-volatile ledger.
Which of the above statements are correct?
(A) Only (I), (II), (III), and (IV)
(B) Only (I), (II), (IV), and (V)
(C) Only (II), (III), (IV), and (V)
(D) All (I), (II), (III), (IV), and (V)

**May/June 2018**

**107.** A marketing team has a large dataset of unclassified demographic data. They want an algorithm to discover distinct population segments based purely on common features and buying habits without any preconceived categories. Which data mining approach is required?
(A) Clustering
(B) Classification

NODIA

an OLAP system.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2013**

**121.** A risk analytics team wants to trace complex event trails and relationships between fraudulent actors. Rather than using standard relational tables, they implement a database specifically designed for graph analytics. Which emerging trend category does this fall under?

(A) Use of commodity servers
(B) Migration to pure OLTP operational structures
(C) Decommissioning of all Extractive Transformation tools
(D) New types of specifically designed DBMS

**Oct/Nov 2021**

**122.** A financial institution wishes to minimize the need to move data back and forth to external systems for analysis. They decide to utilize native SQL, R programming integration, and data mining algorithms directly within their data warehouse. What emerging trend does this represent?

(A) Cloud and Automation
(B) Autonomous database healing
(C) In-database analytics
(D) Physical hardware consolidation

**May/June 2024**

**123.** To manage burgeoning large-scale information without facing integration headaches, an institution purchases a system preconfigured and optimized for specific workloads. This approach is an example of which emerging trend?

(A) The shift to ledger-based DBMS
(B) The adoption of commodity open-source servers
(C) Engineered systems becoming a preferred approach
(D) Virtual Data Warehouse elimination

**Oct/Nov 2008**

**124.** An institution needs to accelerate number-crunching for high-frequency trading reports. They adopt an architecture that processes large data sets directly in system RAM, achieving high performance. Which technology are they adopting?

(A) In-memory technologies
(B) Ledger-based blockchain DBMS
(C) Virtual point-to-point data warehousing
(D) Distributed physical magnetic storage

**May/June 2006**

**125.** An institution's marketing team seeks to establish a comprehensive, 360-degree view of their customer base to improve personalized marketing automation and customer service. What emerging practice enables this initiative?

(A) Downsizing data storage to standalone mobile edge cases
(B) Using real-time analytics to improve CX marketing campaigns
(C) Replacing data warehouses entirely with unstructured raw data lakes
(D) Utilizing classification to forecast macroeconomic turning points

www.nodia.in

Downloaded from www.pdf.tube

(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2011**

**114.** To detect fraudulent claims, a company implements a system inspired by the information processing model of the human brain, utilizing interconnected processing nodes that receive information, process it, and pass states to other nodes. This system is known as a(n):
(A) Expert System User Interface
(B) Artificial Neural Network
(C) Online Transaction Processing System
(D) Data Granularity Matrix

**May/June 2010**

**115.** A bank's database administrators are debating how to store customer names. They consider storing "John Arthur Doe" as a single string versus subdividing it into three fields: First Name, Middle Name, and Last Name. What fundamental characteristic of a data warehouse does this design decision reflect?
(A) Data Non-volatility
(B) Time-variant storage
(C) Virtual integration
(D) Data Granularity

**Oct/Nov 2024**

**116.** Data Mining utilizes specific algorithmic approaches. Consider the following:
I Association links occurrences in a single event, such as items bought in a single visit.
II Classification learns from existing past data that already have been classified.
III Clustering discovers different groupings within the data depending on common features.
IV Forecasting uses statistical methods to build models determining relationships to predict future behavior.
V Sequencing permanently locks historical data arrays into immutable ledgers.
Which of the above correctly define these approaches?
(A) Only (I), (II), and (III)
(B) Only (I), (II), and (IV)
(C) Only (II), (III), and (IV)
(D) All (I), (II), (III), and (IV)

**May/June 2017**

**117.** A multinational retail chain wants to understand natural buying patterns to modify shelf layouts. They analyze transactional data to link the number of items purchased by a customer in a single visit. Which data mining approach are they utilizing?
(A) Forecasting
(B) Classifications
(C) Clusters
(D) Associations

**Oct/Nov 2005**

**118.** Given below are two statements: one is labelled as Assertion (A) and the other is labelled as Reason (R).
Assertion (A): A virtual point-to-point data warehouse strategy minimizes the amount of redundant data that must be loaded and maintained.
Reason (R): It allows end-users to get at operational databases directly using tools, which can put the largest unplanned query load on operational systems.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2020**

**119.** An insurance company decides to automate routine mortgage underwriting decisions. They implement a system built around a Knowledge Base containing thousands of if-then statements provided by experienced underwriters. What technology is the company primarily utilizing?
(A) An Expert System
(B) An Operational Data Store
(C) A Virtual Data Warehouse
(D) A Blockchain Ledger Database

**Oct/Nov 2015**

**120.** Given below are two statements: one is labelled as Assertion (A) and the other is labelled as Reason (R).
Assertion (A): OLAP tools can provide the benefit of increased performance over traditional database access tools.
Reason (R): A great deal of the complex calculation that is required to summarize the data is done long before a query is submitted in

NODIA

May/June 2023

**95.** Given below are two statements: one is labelled as Assertion (A) and the other is labelled as Reason (R).
Assertion (A): Business Intelligence is most effective when it combines external market data with internal company financial and operations data.
Reason (R): This combination provides a more complete picture that creates an intelligence which cannot be derived by any singular set of data.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Oct/Nov 2018

**96.** Retail managers complain that generating reports on live transactional databases slows down point-of-sale systems and provides only current data. The IT department proposes implementing a technology designed for live ad hoc access to summarized, multidimensional historical views. What should they implement?
(A) OLTP (On-Line Transaction Processing)
(B) OLAP (On-Line Analytical Processing)
(C) A traditional RDBMS Normalization Routine
(D) A Point-to-Point Virtual Database

May/June 2007

**97.** The Data Warehouse Architecture contains several distinct layers. Consider the following layers:
I Data Extraction Layer
II ETL Layer
III Data Logic Layer
IV System Operations Layer
V Virtual Network Router Layer
Which of the above represent actual layers defined in the architecture framework?
(A) Only (I), (II), (III), and (V)
(B) Only (I), (II), (III), and (IV)
(C) Only (II), (III), and (IV)
(D) All (I), (II), (III), (IV), and (V)

Oct/Nov 2025

**98.** A large retail bank decides to construct an informational system. They want the new system to serve only the Credit Card division, isolating it from the broader enterprise to focus strictly on local analysis of subject-specific data. Based on data warehouse options, what structure is the bank adopting?
(A) Data Mart
(B) Central Data Warehouse
(C) Operational Data Store (ODS)
(D) Distributed Data Warehouse

May/June 2012

**99.** An insurance company wishes to find hidden patterns in policyholder behavior without relying on explicit rules. They deploy a system that uses historical data to emulate human thought patterns and model behavior dynamically. What subset of artificial intelligence are they applying?
(A) Conventional Procedural Coding
(B) Machine Learning
(C) Extractive Transformation Parsing
(D) Data Cleansing Normalization

Oct/Nov 2014

**100.** Given below are two statements: one is labelled as Assertion (A) and the other is labelled as Reason (R).
Assertion (A): The ETL design phase is rarely a time-consuming phase in a data warehousing project.
Reason (R): In the ETL layer, logic is applied to transform data from a transactional nature to an analytical nature, and data cleansing happens.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2019

**101.** A retail chain identifies a trend where customers buy a crib, and then exactly three months later, purchase baby formula. By linking these events over a period of time, which specific data mining approach is the company exploring?
(A) Sequences

Click Here to Buy book on Amazon

# ANSWERS

NODIA

1. (B) 3 types
The Data Storage Layer within a data warehouse architecture typically encompasses three distinct types of entities based on their scope and specific functionality. These include the Enterprise Data Warehouse, the subject-specific Data Mart, and the Operational Data Store. Each entity serves a unique purpose in managing historical and current information to support varied organizational analytical requirements.

2. (C) By providing a unified 360-degree customer view for sentiment and personalization
Real-time analytics conceptually enhance marketing campaigns by enabling a unified 360-degree view of the customer base. This comprehensive perspective facilitates immediate sentiment analysis and highly personalized interactions. By integrating diverse data streams instantaneously, organizations can respond to consumer behaviors more effectively, ensuring that marketing efforts are both relevant and timely in a competitive business environment.

3. (C) Information describing data stored within the warehouse system
In a data warehouse environment, metadata is precisely defined as information that describes the data stored within the system. It acts as a guide for understanding the structure, origin, and meaning of informational assets. This descriptive data is essential for users and developers to navigate, manage, and utilize the warehouse effectively for reporting and strategic analysis.

4. (C) Management must recognize that maintenance of the data warehouse structure is as critical as any other mission-critical application
Management must recognize that the ongoing maintenance of a data warehouse structure is just as critical as any other mission-critical application. These systems are not temporary measures but long-term strategic assets. Proper oversight ensures data remains consistent, reliable, and capable of meeting evolving organizational needs for informed decision-making across various departments and executive levels.

5. (B) Data lakes store data in raw form, while data warehouses store data in a highly structured and transformed form
Data lakes and data warehouses differ fundamentally in their storage philosophy. Data lakes store vast amounts of information in its raw, unprocessed form, allowing for future flexible analysis. In contrast, data warehouses store data that has been highly structured and transformed to support specific business intelligence and reporting tasks, ensuring high performance and data consistency.

6. (B) It links occurrences within a single event, such as items purchased during one visit
The association approach in data mining focuses on linking occurrences within a single event or transaction. A classic example is identifying items frequently purchased together during a single retail visit. This technique helps businesses understand consumer behavior patterns, allowing for optimized product placement, targeted promotional strategies, and improved inventory management based on observed relationships between different products.

7. (B) Data in jail
The term used to describe billions of bytes of operational data locked within various computer systems and difficult for decision-makers to access is data in jail. This phenomenon highlights the challenge of extracting valuable insights from siloed or legacy environments. Overcoming this barrier is a primary motivation for implementing comprehensive data warehousing and business intelligence solutions.

8. (B) It stores business rules that govern the presentation and appearance of reports
The Data Logic Layer within a data warehouse architecture serves the conceptual function of storing business rules that govern the presentation and appearance of final reports. These rules define how information is displayed to end-users without altering the underlying raw data. This separation ensures that reporting remains

**41.** (A) (II), (IV), (I), (III)
Establishing a virtual data warehouse environment begins with installing data access and management facilities. Once the system is ready, end-users are trained to use these tools for direct data access. Administrators then monitor how these facilities are actually utilized in practice. Finally, based on this usage data, a physical data warehouse is created to support high-frequency analytical requests.

**42.** (C) Data marts operate enterprise-wide, whereas data warehouses focus on departments
It is incorrect to state that data marts operate enterprise-wide while data warehouses focus on departments. In practice, a data warehouse is an enterprise-level repository managing comprehensive information. A data mart is a subset of this data, specifically tailored for a business division or department's needs. The broader the scope of the warehouse, the more value it provides.

**43.** (B) Setting daily operational naming conventions
Artificial Neural Networks have diverse applications, including identifying tax fraud, mortgage underwriting, and verifying bank notes or signatures. These tasks rely on the network's ability to recognize complex patterns. Setting daily operational naming conventions is an administrative or governance task performed by human managers or architects and does not involve the algorithmic pattern-matching capabilities of a neural network.

**44.** (D) Future unrecorded operational projections generated without historical data
The Data Source Layer receives information from existing feeds such as web server logs, internal market research, and third-party demographic data. These sources provide the raw material for the warehouse. Future unrecorded operational projections generated without historical data are not valid sources, as the data warehouse fundamentally relies on existing records to perform historical analysis and support strategic decision-making.

**45.** (C) It delivers information to users via tabular reports, graphical charts, or alerts
The primary role of the Data Presentation Layer is to deliver information to end-users in a usable format. This includes generating tabular reports, graphical charts, and alerts based on the analyzed data. It serves as the interface between the analytical environment and the decision-makers, ensuring that insights are communicated effectively to support strategic goals and day-to-day business oversight.

**46.** (B) Database normalization is identical to subject orientation
Subject orientation in a data warehouse refers to organizing data around key business entities rather than transactional processes. It is incorrect to say that database normalization is identical to subject orientation. Normalization is a technique used in operational databases to reduce redundancy and ensure integrity, whereas subject orientation focuses on consolidating only the necessary information required for effective analytical decision-making.

**47.** (B) When it integrates external market data with internal sources for a complete view
Business Intelligence is considered most effective when it integrates external market data with internal company sources. This combination provides a complete picture that cannot be derived from any single set of data. By merging these perspectives, organizations can gain a competitive advantage, making better-informed decisions regarding strategic directions, product pricing, and how the enterprise will operate in the future.

**48.** (B) End-users typically know exactly what they need as a bare minimum before design begins
It is incorrect to assume that data warehouse users typically know exactly what they need before the design process begins. In reality, requirements are often difficult to define because they involve broad business concepts. Developing robust working prototypes is essential to help users visualize their needs. Designing these systems differs significantly from creating traditional operational systems that focus on specific tasks.

**49.** (A) Migration of all data entirely to paper-based offline ledgers to enhance security
Emerging trends in data warehousing include the use of engineered systems, in-database analytics, and the integration of AI operations with cloud automation. These technologies focus on

Downloaded from www.pdf.tube

17. (A) Designing a data warehouse is quite close to Business Process Reengineering (BPR)
Designing a data warehouse is considered very close to Business Process Reengineering because it often requires rethinking how information is used across the organization. Unlike traditional operational systems, data warehouse design focuses on broad and sometimes difficult-to-define business concepts. Robust working prototypes are typically essential to help users visualize their needs and refine the analytical requirements effectively.

18. (B) 3 broad categories
The end-users of a data warehouse are generally classified into three broad categories based on their analytical needs and roles. These groups include executives and managers seeking strategic insights, power users such as business analysts and engineers performing deep data dives, and support users like clerical staff who handle routine administrative tasks and generate standardized reporting for various departments.

19. (D) Processing data in system RAM to accelerate analytics and actionable reporting
In-memory technologies operate by processing large datasets directly within the system RAM rather than relying on traditional disk-based storage. This approach significantly accelerates data retrieval and analytical processing, enabling near-instantaneous reporting and actionable insights. By eliminating the latency associated with physical hard drives, organizations can handle massive information volumes with high performance and efficiency for real-time applications.

20. (A) When there is a regulatory or statutory obligation to do so
The non-volatile nature of a data warehouse means that data is generally read-only once loaded, serving as a permanent historical record. However, updates or deletions may conceptually occur under specific conditions, such as a regulatory or statutory obligation. This ensures that while the system maintains historical integrity, it can still comply with legal requirements like data privacy laws.

21. (C) They utilize components across multiple databases, often increasing redundancy and complexity
Distributed Data Warehouses are characterized by components spread across multiple physical databases, often utilizing local area networks. This structure typically leads to increased data redundancy and more complex updating processes compared to centralized models. However, it allows for decentralized decision-making by pushing data closer to the specific business divisions or geographic locations where the information is most relevant.

22. (C) Up to 10 years
Data warehouses are designed to store historical information over a significantly long time horizon, typically representing up to ten years of enterprise data. This long-term perspective is essential for identifying trends, performing complex forecasting, and conducting detailed data mining. In contrast, operational systems focus on much shorter windows, usually covering only current day-to-day transactional activities within the organization.

23. (D) Operational systems focus on a single area for day-to-day operations, whereas informational systems span multiple areas for planning and forecasting
The core conceptual difference between operational and informational systems lies in their scope and purpose. Operational systems focus on a single functional area for day-to-day tasks like order entry. Informational systems, however, span multiple areas across the enterprise to support high-level planning and forecasting. They integrate diverse data to help decision-makers understand how the organization will operate in the future.

24. (D) They are single databases using advanced RDBMS for specific functional areas
Central Data Warehouses are characterized as single databases built around advanced Relational Database Management Systems. These repositories are typically designed to support specific functional areas or the entire enterprise by consolidating information into one physical location. This centralized approach simplifies data management and provides a consistent

NODIA

**75.** (D) All (I), (II), (III), and (IV)
A data warehouse is defined by four essential characteristics that distinguish it from traditional operational systems. It is subject-oriented, focusing on key business entities, and integrated, meaning inconsistencies are unified. It is also time-variant, maintaining snapshots over a long historical horizon, and non-volatile, ensuring that data is generally read-only once loaded into the informational environment for strategic analysis.

**76.** (D) P-2, Q-4, R-1, S-3
The fundamental characteristics of a data warehouse ensure its effectiveness for analysis. Subject-orientation involves gathering only the necessary objects for decision-making. Integration requires eliminating inconsistencies like naming conventions across sources. Time-variance means the data represents a long historical horizon, often up to ten years. Non-volatility signifies that the data is read-only and cannot be updated once it is stored.

**77.** (D) All (I), (II), and (III)
An expert system is composed of three essential subsystems that work together to provide automated advice. These include the user interface, which allows non-experts to interact with the system, and the knowledge base, which stores specialized facts and rules. The inference engine acts as the reasoning component, applying those rules to deduce new facts from the provided information.

**78.** (D) P-3, Q-4, R-2, S-1
Emerging trends in data warehousing leverage new technologies to improve performance. Physical and logical consolidation uses virtualization and multi-tenancy to reduce costs. Real-time analytics provides a 360-degree customer view for sentiment analysis. Engineered systems offer preconfigured hardware appliances optimized for specific workloads. In-memory technologies process large datasets within system RAM to achieve high-speed performance for demanding analytical tasks.

**79.** (B) Only (II)
Expert systems utilize a knowledge base and an inference engine to solve complex problems through reasoning, typically using if-then rules. This statement is correct. However, it is incorrect to say that machine learning requires strict, explicit procedural rules. In fact, machine learning focuses on finding patterns in historical data without being explicitly programmed with rules for every possible scenario.

**80.** (D) Edge use cases DBMS - Requires massive centralized commodity server clusters
It is incorrect to associate edge use case DBMS with a requirement for massive centralized commodity server clusters. In reality, edge computing focuses on processing data near the source, such as on mobile devices or local sensors, rather than centralizing it. Other trends like autonomous databases, time-series databases for event trails, and blockchain-inspired ledger systems are accurately paired.

**81.** (D) All (I), (II), (III), and (IV)
Artificial Neural Networks have a wide range of real-world business applications across various domains. These include mortgage underwriting, forecasting foreign exchange rates, and classifying consumer spending patterns. They are also used in human resources to determine personnel resource requirements. These tasks leverage the network's ability to model complex, non-linear relationships and recognize patterns in large, multifaceted datasets effectively.

**82.** (A) P-4, Q-1, R-2, S-3
Expert systems are composed of specific components that facilitate automated reasoning. The inference engine applies rules to known facts to deduce new information. The knowledge base serves as a collection of specialized facts and rules. The user interface allows non-expert users to query the system and receive advice. A rule-based system uses if-then statements to act upon assertions.

**83.** (D) P-3, Q-4, R-1, S-2
Artificial Neural Networks are applied across many business domains. In accounting, they are used to identify tax fraud. Within finance, they assist in mortgage underwriting decisions. Marketing departments utilize them to classify consumer spending patterns for targeted strategies. In human resources, these systems help determine personnel resource requirements,

Click Here to Buy book on Amazon

**33.** (B) The ETL Layer is exclusively used for storing tabular and graphical reports for end-users
The ETL Layer is not used for storing final reports; instead, it is where data cleansing and complex transformations occur to prepare information for analysis. The Presentation Layer is actually responsible for delivering reports to end-users. ETL design is often the most time-consuming phase of a project because it involves applying business logic to convert transactional data into useful insights.

**34.** (D) The biological information processing model of the interconnected human brain
Artificial Neural Networks are fundamentally inspired by the biological information processing model of the human brain. They consist of interconnected processing nodes, or neurons, that receive, process, and pass information. This structure allows the system to learn from data and identify complex patterns, making it highly effective for tasks such as image recognition, fraud detection, and financial market forecasting.

**35.** (A) Data Divestment Layer
General data warehouse architecture is organized into several distinct functional layers. These typically include the Data Source Layer, Staging Area, ETL Layer, Data Storage Layer, Data Logic Layer, Data Presentation Layer, Metadata Layer, and System Operations Layer. Each layer plays a specific role in the data flow process. A Data Divestment Layer is not a standard component of this architectural framework.

**36.** (A) Reducing costs via virtualization and multi-tenancy instead of linear hardware scaling
The key benefit of physical and logical consolidation in growing data warehouses is the reduction of costs through technologies like virtualization and multi-tenancy. This approach prevents storage and management expenses from increasing linearly with data volume. By optimizing resource usage and using advanced compression, organizations can manage expanding information assets more sustainably without the need for constant, expensive hardware additions.

**37.** (A) Data lakes store highly structured data exclusively, whereas data warehouses manage only raw data
It is incorrect to say that data lakes store only structured data and data warehouses manage only raw data. In reality, data lakes are designed to store information in its raw form, including unstructured data. Conversely, data warehouses store data that has been highly structured and transformed for specific analytical purposes. Big data encompasses both structured and unstructured formats.

**38.** (D) System architects (database administrators, network engineers)
Data warehouse end-users are typically categorized into three groups: executives and managers, power users like analysts and engineers, and support users such as clerical staff. These categories represent the individuals who consume the information for decision-making and reporting. System architects, including database and network engineers, are responsible for building and maintaining the infrastructure rather than being the end-users.

**39.** (D) To provide a long time horizon intended for data mining and forecasting
Storing time-variant data in a data warehouse is primarily intended to provide a long historical time horizon, often spanning several years. This allows organizations to track changes over time, identify long-term trends, and perform advanced data mining and forecasting. Unlike operational systems that focus on current status, time-variant storage captures snapshots of data as it evolves for strategic analysis.

**40.** (D) Association specifically builds statistical models to classify risk based exclusively on predefined segments
Association in data mining links occurrences within a single event, such as items bought together, rather than building statistical models to classify risk based on predefined segments. Risk classification is typically handled by the classification approach. Forecasting models relationships to predict future behavior, while clustering discovers groupings in unclassified data. Each technique serves a unique purpose in uncovering informational patterns.

Downloaded from www.pdf.tube

**58.** (A) In-database analytics require significant data movement back and forth to other systems for analysis
In-database analytics is designed to simplify analysis by performing tasks directly within the warehouse using native tools, thereby reducing the need for significant data movement between systems. It is incorrect to say it requires more movement. Other trends include physical and logical consolidation through virtualization, the use of high-performance in-memory technologies, and adopting commodity servers to minimize vendor lock-in.

**59.** (C) An enterprise-wide framework for managing informational data within the organization
Data warehousing is best described as an enterprise-wide framework for managing informational data within an organization. It is not limited to clerical tasks or day-to-day transactional processing. Instead, it consolidates data from across the enterprise to support analysis and strategic planning. This framework provides a long-term historical perspective, enabling decision-makers to identify trends and perform complex business modeling.

**60.** (B) Ledger Base Store (LBS)
Based on scope and functionality, the Data Storage Layer in a data warehouse architecture typically contains three distinct types of entities: the Data Warehouse, the Data Mart, and the Operational Data Store. Each serves a specific analytical or operational reporting purpose. A Ledger Base Store is not identified as one of these standard entities within the structural framework of the layer.

**61.** (C) P-3, Q-1, R-2, S-4
Data mining approaches serve various analytical needs. Associations link occurrences within a single event, like items bought together. Classifications use past, pre-grouped examples to categorize new data, such as credit card proposals. Clustering discovers natural groupings within unclassified data based on common features. Forecasting builds statistical models, such as using financial ratios to predict future behavior like bankruptcy for regional suppliers.

**62.** (A) Only (I)
Designing a data warehouse is closely related to Business Process Reengineering because it often involves fundamentally rethinking how information supports organizational goals. However, the ideal design strategy is not strictly top-down. Instead, an evolutionary outside-in approach is often preferred, starting with user needs and prototyping to refine requirements, as informational users frequently do not know their exact needs beforehand.

**63.** (A) P-3, Q-4, R-1, S-2
Each layer in a data warehouse architecture has a specific function. The Data Source Layer provides feeds from various operational and external systems. The Staging Area holds data before cleansing and transformation. The Data Logic Layer stores business rules that dictate the final appearance of reports. The Metadata Layer contains information describing the data and structure within the entire warehouse system.

**64.** (A) Only (I) and (II)
OLAP applications provide significant advantages by enabling managers to model complex problems that are beyond the capacity of traditional, less flexible systems. They also increase productivity by making business users more self-sufficient, reducing their reliance on IT for every analytical change. However, OLAP tools do not replace the data warehouse; rather, they rely on it to provide historical, multidimensional views.

**65.** (A) Metadata Layer - Stores rules to map, translate, and transform data sources
The Metadata Layer is correctly matched with the function of storing rules used to map, translate, and transform data from sources to warehouse elements. This layer acts as a repository for descriptive information about the warehouse structure. Other layers like ETL handle the actual cleansing, while the Data Presentation Layer manages the delivery of graphical reports directly to end-users.

**66.** (A) Only (I), (II), and (III)
Business Intelligence encompasses several key applications and technologies designed to support strategic decision-making. These include Decision Support Systems, Online Analytical Processing, and data mining techniques. Each

NODIA

improving performance and efficiency. Migrating data entirely to paper-based offline ledgers is not a recognized trend, as it would be contrary to the goals of rapid access, advanced analytics, and large-scale information management.

**50.** (C) Decentralized Edge Warehouses
When evaluating data warehouse options based on redundancy, enterprises typically consider three levels. These are virtual or point-to-point data warehouses, central data warehouses, and distributed data warehouses. Each option offers different trade-offs regarding data duplication and maintenance complexity. Decentralized edge warehouses are not identified as one of these three standard structural levels for evaluating enterprise-wide data redundancy strategies.

**51.** (D) Because ML algorithms generate proactive insights that improve operational efficiency
AI Operations and Cloud integration are becoming essential because machine learning algorithms can generate proactive insights that significantly improve operational efficiency. These technologies automate complex backend tasks and provide advanced analytical capabilities that legacy systems cannot match. By leveraging the cloud, organizations can scale their informational infrastructure while using AI to refine data processes and enhance strategic decision-making.

**52.** (D) It eliminates all unplanned query loads on operational systems entirely
The virtual data warehouse strategy provides flexibility and minimizes redundant data by allowing direct access to operational databases. However, it is incorrect to say it eliminates unplanned query loads. In fact, this approach can put a significant and unpredictable load on the primary operational systems, which may impact their performance for day-to-day transactional tasks and essential business functions.

**53.** (C) Marketing planning system
Operational backbone systems are computerized applications that perform day-to-day tasks essential for running an enterprise. These include order entry, inventory management, and payroll systems. A marketing planning system is categorized as an informational system rather than an operational one. Planning systems focus on long-term strategy and analysis across various business areas, rather than the immediate execution of routine transactions.

**54.** (C) Building populated prototype warehouses based on analyzed user population needs
The ultimate optimal strategy for developing a data warehouse involves building populated prototype warehouses based on a thorough analysis of user population needs and questions. This evolutionary approach ensures that the system aligns with actual business requirements. By focusing on user input and iterative development, organizations can create more effective informational environments that provide meaningful insights for strategic decision-making.

**55.** (A) Transformation Engine
An Expert System is fundamentally divided into three main subsystems: the knowledge base, the inference engine, and the user interface. Together, these components allow the system to store expert facts, reason through logic, and interact with users. A transformation engine is not a recognized part of this structure; it is more typically associated with ETL processes in data warehousing.

**56.** (A) It houses the operational transaction processing engine for day-to-day operations
The Metadata Layer is where information about the data stored within the data warehouse system is housed, including logical data models and navigational rules. It is incorrect to claim it houses the operational transaction engine for day-to-day tasks. Such engines are part of the operational systems, while the metadata layer serves as a directory and guidebook for the warehouse.

**57.** (A) To provide a common area for data to reside before scrubbing and transformation
The primary purpose of a staging area in the data warehouse architecture is to provide a common location where data resides before it undergoes scrubbing and transformation. This temporary buffer makes subsequent processing easier and more organized. By holding raw data in the staging area, the system can apply necessary cleansing and business rules more efficiently before loading it into storage.

Click Here to Buy book on Amazon

consistent and easily adjustable as business requirements and user preferences evolve.

**9.** (B) Operational logs including ETL status, system performance, and access history
The System Operations Layer is responsible for managing operational logs that track the status of ETL jobs, system performance, and user access history. This layer ensures the overall health and security of the data warehouse environment. Monitoring these metrics allows administrators to optimize performance, troubleshoot issues, and maintain an audit trail for compliance and resource management purposes.

**10.** (B) 10X
Oracle Hybrid Columnar Compression is an advanced storage method designed to match organizational data growing at a rate of ten times. This technology enables organizations to store significantly higher volumes of valuable information without experiencing proportional increases in storage costs. It achieves this by using highly efficient compression algorithms that optimize both performance and physical space requirements.

**11.** (D) They are preconfigured hardware optimized for specific workloads to ensure performance
Engineered systems in data warehousing consist of preconfigured hardware and software components that are specifically optimized for intensive workloads. These integrated appliances ensure high performance by minimizing compatibility issues and maximizing processing efficiency. This approach has become a preferred method for managing large-scale information environments where traditional, decentralized server configurations may struggle to meet modern analytical demands.

**12.** (C) A system using historical data to find patterns without explicit rules
Machine Learning is accurately defined as a system that utilizes historical data to identify complex patterns and relationships without relying on explicit, hard-coded procedural rules. By learning from examples, these algorithms can make predictions and model behaviors dynamically. This field of artificial intelligence is essential for uncovering insights in large datasets where traditional logic-based systems would be insufficient.

**13.** (A) Clustering groups unclassified data, while Classification learns from pre-grouped examples
Clustering and classification represent two distinct data mining techniques. Clustering focuses on discovering natural groupings within unclassified data based on common features or attributes. Conversely, classification relies on learning from past examples that have already been grouped or categorized. While clustering explores data to find new segments, classification uses known patterns to assign new data points to existing categories.

**14.** (C) The data focuses on business subjects by gathering only specific objects for analysis
The subject-oriented characteristic of a data warehouse implies that data is organized around specific business subjects rather than individual transactional applications. This approach involves gathering only the necessary objects and information beneficial for analytical decision-making. By focusing on subjects like customers, products, or sales, the warehouse provides a consolidated view that supports strategic planning across the entire enterprise.

**15.** (D) The Inference Engine applies rules to facts to deduce new facts via reasoning
An Expert System is composed of several subsystems, including the Inference Engine. This specific component performs the reasoning function by applying knowledge rules to known facts to deduce new information. It simulates the human decision-making process by using logic, typically in the form of if-then statements, to provide answers or guidance in place of a human specialist.

**16.** (A) The level of details considered in a model or decision-making process
Data granularity in the context of a data warehouse refers to the specific level of detail represented within a data model or decision-making process. High granularity means data is stored at a very detailed level, such as individual transactions. Choosing the appropriate granularity is essential for balancing the need for deep analysis with system performance and storage efficiency requirements.

NODIA

of these tools helps organizations analyze historical data and identify trends. Automated Teller Machine switching systems, however, are operational transaction processing systems and are not classified as informational business intelligence applications for analysis.

**67.** (A) (II), (IV), (I), (III)
The typical sequential flow of data in a warehouse architecture starts with the Data Extraction Layer, where raw information is gathered. Next, the ETL Layer cleanses and transforms this data. The Data Logic Layer then applies business rules to govern the information's structure. Finally, the Data Presentation Layer delivers the processed information to end-users through various reporting and visualization tools.

**68.** (A) Only (I)
The term data in jail refers to the challenge of accessing vast amounts of operational data trapped within isolated legacy systems. This makes strategic analysis difficult for executives. However, it is incorrect to say that operational systems are never maintained. In fact, these systems are essential to the business backbone and are frequently enhanced, rewritten, and updated to meet ongoing organizational needs.

**69.** (A) Only (I) and (II)
The metadata component of a data warehouse provides a critical description of the system's structure and contents, often including a detailed data dictionary. It also stores the rules necessary to map, translate, and transform data from various sources. While essential for system navigation, metadata does not function as a graphical interface for day-to-day transactional tasks performed by end-users.

**70.** (C) P-3, Q-2, R-4, S-1
Modern data environments utilize various database technologies and methods. NoSQL databases like MongoDB and Redis offer flexibility for unstructured data. Ledger-based systems, such as Amazon QLDB or blockchain, provide immutable transaction records. Engineered systems are integrated hardware appliances optimized for specific workloads. Advanced data compression methods, like Hybrid Columnar Compression, allow organizations to manage large-scale data growth efficiently and cost-effectively.

**71.** (A) Only (I), (II), and (III)
Recognized trends in data warehousing include the need to handle diverse traffic from IoT and social media through more capable systems. Physical and logical consolidation via multi-tenant databases helps reduce costs, while in-database analytics simplify processing using native SQL and R integration. However, shifting entirely away from backend databases towards purely volatile memory caches is not a standard emerging trend.

**72.** (B) P-2, Q-4, R-3, S-1
Data systems serve various user types across an organization. Power users, such as analysts and engineers, perform deep data analysis. Support users, including clerical staff, handle administrative tasks and routine reporting. Executives use information to make strategic decisions and set broad organizational directions. Operational users run the day-to-day transaction systems, such as order entry and payroll, that form the backbone.

**73.** (B) Only (II)
Distributed data warehouses are designed to push decision-making down to lower organizational levels, though they typically involve higher redundancy and more complex updating processes. It is incorrect to describe central data warehouses as relying exclusively on manual flat files from a single system. Instead, central warehouses use advanced relational database management systems to consolidate information into a single, highly structured physical repository.

**74.** (C) OLAP - Designed for live ad hoc data access and historical decision-making
The correct distinction between OLAP and OLTP is that OLAP is specifically designed for live ad hoc access to summarized, multidimensional historical data for strategic decision-making. OLTP, conversely, is focused on processing current day-to-day transactional data efficiently. While OLTP supports the immediate operations of an enterprise, OLAP provides the analytical depth required to identify long-term trends and performance variances.

Downloaded from www.pdf.tube

source of truth for analytical queries and strategic reporting across the organization.

**25.** (B) OLAP analyzes historical data for decisions, while OLTP processes current transactions online
OLAP and OLTP serve distinct roles in data management. OLTP systems are designed to process current transactions online, facilitating day-to-day business operations efficiently. In contrast, OLAP focuses on analyzing historical data to support strategic decision-making. OLAP tools provide multidimensional views and complex calculations, allowing users to identify trends and perform sophisticated modeling that traditional transactional systems cannot support.

**26.** (D) A strategy enabling direct user access to operational data via a network
A Virtual Data Warehouse is an operational strategy that enables end-users to access operational data directly via a network using specialized tools. Instead of creating a separate physical repository, this approach provides a logical view of the information. It offers flexibility and minimizes data redundancy, though it can place significant unplanned query loads on the primary operational database systems.

**27.** (A) BI is most effective when it combines data derived from the market (external data) with data from company sources (internal data)
Business Intelligence is considered most effective when it integrates data derived from the market with information from internal company sources. This combination of external and internal data provides a complete picture that cannot be achieved through a single data set. By merging these perspectives, organizations can make more informed strategic decisions regarding product positioning, pricing, and overall market competitiveness.

**28.** (A) If-then statements
A rule-based system, often used in expert systems, relies on specific if-then statements to provide answers or guidance. These statements represent the knowledge of human experts and are used to deduce new facts from known assertions. By following these logical rules, the system can solve complex tasks and offer advice in a manner that simulates human reasoning processes.

NODIA

**29.** (C) They are the computerized backbone systems performing day-to-day enterprise tasks.
Operational systems are designed to manage the routine activities of an organization, such as sales processing, payroll, inventory control, customer transactions, and employee records. These systems ensure smooth daily operations by processing large volumes of real-time data quickly and accurately. They support operational-level employees and managers in carrying out regular business functions efficiently. Unlike analytical or strategic systems, operational systems mainly focus on immediate transaction processing and organizational workflow management.

**30.** (D) Inconsistencies like naming and encoding must be unified across source systems
To achieve the integrated characteristic of a data warehouse, inconsistencies across various source systems must be unified. This process involves standardizing naming conventions, data encoding, and physical attributes. Integration ensures that data from disparate operational environments is combined into a coherent and consistent format, which is essential for accurate enterprise-wide analysis and reporting within the informational environment.

**31.** (C) It guarantees high-quality data outputs even if the existing operational data is of poor quality
Building a copy of operational data is a simple and fast strategy for establishing a data warehouse. However, it does not guarantee high-quality outputs if the source data is poor. If the existing operational data contains errors or inconsistencies, the copied version will inherit those issues. Successful implementation requires careful planning regarding data quality and user access requirements.

**32.** (B) Compilations
In the field of data mining, several major approaches are used to uncover patterns and relationships within large datasets. These include associations, classifications, clusters, forecasting, and sequencing. Each method serves a specific analytical purpose, such as identifying items bought together or predicting future behavior. Compilations is not recognized as a standard algorithmic approach in the context of data mining.

showcasing the versatility of neural networks in solving complex organizational problems.

**84.** (B) Only (I) and (III)
Building a copy of operational data is a strategy that offers the advantages of being simple and fast to implement. However, it can lead to significant problems if the existing data is of poor quality or if access has not been properly planned. It does not eliminate the need for storage layers, as the copy itself must be maintained.

**85.** (C) Both (I) and (II)
Both statements regarding the staging and ETL layers are correct. The staging area serves as a temporary location where data sits before it undergoes scrubbing and transformation. The ETL layer is then used to perform data cleansing and apply the logic necessary to transform information from a transactional format into a structure suitable for multidimensional analytical reporting and strategic analysis.

**86.** (B) P-4, Q-2, R-3, S-1
Organizations have several options for managing data redundancy. A virtual data warehouse allows users to access operational databases directly through network tools. A central data warehouse is a single physical database built around advanced RDBMS. Distributed data warehouses involve components spread across different physical locations, while data marts are department-level repositories that contain subject-specific data for localized analytical needs.

**87.** (D) All (I), (II), (III), and (IV)
The Data Source Layer receives information from a variety of internal and external feeds. Valid sources include internal departmental data such as HR and marketing records, as well as web server browsing logs. Additionally, market research data and third-party demographic census information are integrated. These diverse inputs provide the necessary raw material for comprehensive enterprise analysis and strategic decision-making.

**88.** (B) P-3, Q-1, R-2, S-4
Business Intelligence supports various decision-making levels. Basic operating decisions involve product positioning and pricing. Strategic decisions focus on the broadest priorities, goals, and directions of the organization. To make these choices, BI uses external data derived from the market and internal data such as financial and operations records. Integrating these sources provides the intelligence necessary for effective planning.

**89.** (B) Only (I) and (III)
Informational systems are designed to support major strategic decisions by analyzing how an enterprise will operate in the future. These systems typically span multiple functional areas across the organization, requiring large volumes of related operational data to provide a comprehensive view. Unlike operational systems, which focus on a single area for day-to-day tasks, informational systems integrate diverse data for planning.

**90.** (A) Classifications - Predicting bankruptcy using unclassified demographic data
It is incorrect to describe classification as predicting bankruptcy using unclassified demographic data. Classification relies on learning from past examples that have already been categorized. Clustering is the approach used for discovering groupings in unclassified data. Associations link occurrences within a single event, and forecasting uses statistical models to predict future behavior based on established relationships between various parameters.

**91.** (D) Assertion (A) is false, but Reason (R) is true.
The assertion that database normalization is identical to subject orientation is false. Normalization is a technical process used in operational databases to reduce redundancy. In contrast, subject orientation focuses on organizing data around specific business concepts for analysis. However, the reason is true, as subject orientation indeed refers to gathering only the necessary objects beneficial for strategic decision-making processes.

**92.** (C) Data Logic Layer
The Data Logic Layer is responsible for storing business rules that dictate how reports are presented and formatted for end-users. In this scenario, rules for coloring negative balances are housed here. This layer allows organizations to customize the visual appearance of information

Click Here to Buy book on Amazon

# CHAPTER 08
# E-Learning Environment

Oct/Nov 2023

**1.** In which year was version 1.0 of the Experience API (Tin Can API) finalized?
(A) 2011
(B) 2016
(C) 2020
(D) 2013

May/June 2011

**2.** How does Application sharing in a Virtual Classroom differ from a traditional classroom?
(A) Shared applications are technically impossible to implement in Virtual Classrooms
(B) Every student must purchase a separate license for each shared software tool
(C) The application need not be installed on every student's PC, unlike a traditional lab setting
(D) The application view is restricted solely to the instructor in the Virtual Classroom

Oct/Nov 2012

**3.** What does a Learning Management System (LMS) primarily manage?
(A) The internal authoring and automated aggregation of digital instructional components
(B) The technical metadata specifications required for cataloging granular learning objects
(C) Learning processes including class scheduling, catalog creation, and learner registration
(D) The physical storage and logistics for the distribution of printed training materials

May/June 2015

**4.** Which statement accurately reflects Bloom's Taxonomy?
(A) A framework that categorizes educational objectives into four distinct domains
(B) A model where the Psychomotor domain relates specifically to mental skills
(C) A 1956 model dividing objectives into Cognitive, Affective, and Psychomotor
(D) A technical formatting standard for the delivery of digital learning content

Oct/Nov 2013

**5.** What does LCMS rendering of content and tracking of learners' bookmarks and test scores enable?
(A) It allows the immediate printing of completion certificates
(B) It allows the data to be passed back to the LMS for reporting purposes
(C) It deletes the data once the learner logs out
(D) It prevents the learner from retaking the course

May/June 2008

**6.** Which statement about the ADDIE model is correct?
(A) A linear sequence where phases end permanently once implementation is finished
(B) A cyclical loop where the five phases are continually and regularly repeated
(C) An implementation phase that focuses on setting goals and choosing approaches
(D) An evaluation phase that serves as the very first step in the design process

Oct/Nov 2017

**7.** What is the definition of e-Learning?
(A) A method of traditional instruction utilizing modern physical textbooks in classrooms
(B) Learning and teaching delivered through electronic media, particularly the Internet
(C) A correspondence-based distance learning approach reliant on printed materials
(D) A conceptual framework for the systematic design of physical classroom curricula

NODIA

May/June 2006

**8.** In instructional design, what does the concept of "spiral organization" imply?
(A) A cyclical method of repeating the same core content indefinitely

automation and inventory planning based on the predicted timing of consumer needs.

**102.** (D) All (I), (II), (III), (IV), and (V)
Several recognized emerging trends are currently shaping the future of data warehousing. These include real-time analytics for customer sentiment, the use of optimized engineered systems, and advanced compression methods like Hybrid Columnar Compression. Additionally, in-memory technologies enhance performance by processing data in RAM, while AI operations and cloud integration automate backend tasks to generate actionable insights and improve operational efficiency.

**103.** (B) Staging Area
The staging area is the architectural layer that serves as an interim storage location for raw data before complex transformations are applied. It provides a common area for data to reside, which simplifies subsequent cleansing and analytical processing. By routing incoming data here first, the organization ensures that information is organized and prepared properly before being loaded into the storage layer.

**104.** (D) Assertion (A) is false, but Reason (R) is true.
The assertion is false because clustering is used for discovering natural groupings in unclassified data, rather than assuming past examples are already categorized. The reason is true, as clustering focuses on identifying population segments based on common features or buying habits within datasets that lack predefined labels. This approach allows for the discovery of new and unexpected informational patterns.

**105.** (C) Forecasting
The finance department is using the forecasting approach by building statistical models to determine the relationship between financial ratios and the likelihood of future bankruptcy. This data mining technique uses historical variables to predict future outcomes and behaviors. It is an essential tool for risk management, allowing organizations to anticipate potential issues and take proactive measures to mitigate financial loss.

**106.** (A) Only (I), (II), (III), and (IV)
Several statements regarding data redundancy are correct. Virtual warehouses minimize redundant data but increase operational load. Central warehouses consolidate data for functional areas into physical databases. Distributed systems push decision-making to local levels and often involve complex loading processes. However, it is incorrect to say point-to-point systems centralize all external data into a non-volatile ledger; they are typically virtualized and decentralized.

NODIA

**107.** (A) Clustering
To discover distinct population segments based purely on common features and buying habits within an unclassified dataset, the clustering approach is required. This technique groups data points together based on their inherent similarities without any preconceived categories. It is particularly useful for market segmentation, allowing companies to identify unique customer groups and tailor their products and promotional strategies accordingly.

**108.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Both the assertion and the reason are true, and the reason provides the correct explanation. The non-volatile characteristic of a data warehouse means that once data is loaded, it is generally read-only. This prevents users from updating or deleting historical records, ensuring data integrity for long-term analysis. Updates are only permitted under exceptional circumstances, such as fulfilling specific regulatory obligations.

**109.** (D) System Operations Layer
The System Operations Layer provides the capability to maintain logs of ETL job status and user access history. This layer is essential for monitoring system performance and ensuring security within the data warehouse environment. By tracking these operational metrics, IT teams can troubleshoot processing issues, audit user activity, and optimize the infrastructure to support the organization's ongoing analytical needs.

**110.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Both the assertion and the reason are true, and the reason correctly explains the assertion. Physical and logical consolidation of data warehouses

without modifying the underlying data or the transformation logic used to prepare it for analytical reporting purposes.

**93.** (D) All (I), (II), (III), (IV), and (V)
Successful data warehouse development requires several strategic considerations. These include building prototypes based on user needs and adopting an evolutionary approach. The design strategy is often outside-in, reflecting broad business concepts. Careful management is essential, and implementation often creates new demands on operational systems for better, consistent data. Each of these factors contributes to the long-term success of the informational environment.

**94.** (C) Classification
When an organization uses past credit evaluations that are already categorized into specific risk groups to evaluate new proposals, they are performing a classification activity. This data mining approach learns from pre-grouped examples to assign new data points to existing categories. It is highly effective for tasks like risk management, where historical patterns are used to guide future decisions.

**95.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Both the assertion and the reason are true, and the reason correctly explains the assertion. Business Intelligence reaches its full potential when it integrates external market data with internal company information. This combination creates a more complete and actionable picture of the business environment. The resulting intelligence provides strategic insights that could not be derived from any single dataset alone.

**96.** (B) OLAP (On-Line Analytical Processing)
Online Analytical Processing is the technology designed specifically for live, ad hoc access to summarized and multidimensional historical views of data. Unlike OLTP, which focuses on current transactions, OLAP allows managers to perform complex analysis and identify trends without slowing down operational systems. It provides the flexibility and performance necessary for high-level strategic decision-making and reporting across various departments.

**97.** (B) Only (I), (II), (III), and (IV)
The standard data warehouse architecture framework includes several defined layers. These include the Data Extraction Layer, the ETL Layer for cleansing and transformation, the Data Logic Layer for business rules, and the System Operations Layer for monitoring performance and logs. A Virtual Network Router Layer is not a recognized component of this specific architectural model for managing informational data.

**98.** (A) Data Mart
A data mart is the structure adopted when a system is designed to serve a specific business division, such as the credit card department, and focuses on local analysis of subject-specific data. Unlike a central data warehouse that covers the entire enterprise, a data mart is more limited in scope, making it highly targeted and easier to manage for departments.

**99.** (B) Machine Learning
Machine Learning is the subset of artificial intelligence that focuses on finding hidden patterns in data without relying on explicit, hard-coded rules. By using historical data to model behavior dynamically, these systems can emulate human thought patterns and improve their performance over time. This technology is particularly useful for complex tasks like fraud detection and behavior analysis in large datasets.

**100.** (D) Assertion (A) is false, but Reason (R) is true.
The assertion that the ETL design phase is rarely time-consuming is false, as this stage is often the most labor-intensive part of a data warehousing project. However, the reason is true because the ETL layer is where data cleansing occurs and business logic is applied to transform information from a transactional nature to an analytical format for storage.

**101.** (A) Sequences
By identifying a pattern where one purchase is followed by another specific purchase over a defined period, the company is utilizing the sequences data mining approach. This technique links events through time, helping businesses understand customer progression and life stages. Such insights allow for more effective marketing

Downloaded from www.pdf.tube

is a drawback rather than an explanation for redundancy.

**119.** (A) An Expert System
An expert system is being utilized when a company automates decisions using a knowledge base of if-then statements derived from human experts. This technology simulates the reasoning process of a specialist to solve complex tasks, such as mortgage underwriting. By applying these predefined rules to specific facts, the system provides consistent and reliable guidance in place of a human underwriter.

**120.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Both the assertion and the reason are true, and the reason correctly explains the assertion. OLAP tools provide superior performance compared to traditional query tools because complex calculations and summarizations are performed in advance. By pre-calculating these values before a query is ever submitted, the system can deliver near-instantaneous results, enabling faster and more efficient multidimensional analysis for strategic decision-making.

**121.** (D) New types of specifically designed DBMS
Implementing a database specifically designed for graph analytics to trace complex relationships falls under the emerging trend of new types of specifically designed DBMS. These systems move beyond traditional relational models to handle specialized data structures and complex event trails more effectively. Other examples of this trend include time-series databases for event trails and ledger-based systems inspired by blockchain technology.

**122.** (C) In-database analytics
Utilizing native SQL, R programming integration, and data mining algorithms directly within the data warehouse represents the trend of in-database analytics. This approach eliminates the need to move large volumes of data back and forth to external systems for processing. By performing analysis where the data resides, organizations can simplify their analytical workflows, improve performance, and achieve more timely insights.

**123.** (C) Engineered systems becoming a preferred approach
The adoption of preconfigured systems that are optimized for specific workloads is an example of the trend where engineered systems are becoming a preferred approach. These integrated hardware and software appliances are designed to deliver high performance while reducing integration challenges. This method allows organizations to manage large-scale informational requirements more efficiently than using traditional, decentralized server and software configurations.

NODIA

**124.** (A) In-memory technologies
In-memory technologies are being adopted when an architecture processes large data sets directly within system RAM to achieve high-speed performance. This approach is significantly faster than traditional disk-based processing, making it ideal for time-sensitive tasks like high-frequency trading reports. By eliminating the latency of physical drives, organizations can perform intensive number-crunching and deliver near-instantaneous analytical results for strategic use.

**125.** (B) Using real-time analytics to improve CX marketing campaigns
The practice of establishing a comprehensive 360-degree view of the customer base to improve marketing automation is enabled by real-time analytics. This approach allows organizations to perform immediate sentiment analysis and personalization. By integrating various customer touchpoints instantaneously, businesses can respond more effectively to consumer behaviors, ensuring that marketing campaigns and customer service interactions are both relevant and timely.

www.nodia.in

(A) A protocol using statements formatted as 'actor, verb, and object'
(B) A system that stores data exclusively within a local content management system
(C) A method designed to manage the physical inventory of traditional classrooms
(D) An early and now obsolete version of the SCORM technical specification

**May/June 2010**

**18.** What is the minimum connection speed required for ensuring the highest possible performance of adaptive video bandwidth in a Virtual Classroom?
(A) 480 kbps
(B) 128 kbps
(C) 256 kbps
(D) 512 kbps

**Oct/Nov 2011**

**19.** Why do organizations adopt gamification in their learning platforms?
(A) The complete replacement of human instructors with automated game engines
(B) The reduction of network bandwidth required for streaming video-based learning
(C) The distribution of physical rewards to students for completing assignments
(D) Motivating learners by presenting their training as an engaging 'play thing'

**May/June 2009**

**20.** Which SCORM objective refers to the ability to increase efficiency and productivity by reducing the time and costs involved in delivering instructional content?
(A) Affordability
(B) Accessibility
(C) Adaptability
(D) Durability

**Oct/Nov 2019**

**21.** Which statement regarding the SCORM Conformance Test Suite is correct?
(A) A restricted software suite available only to accredited government agencies
(B) A diagnostic tool used exclusively for testing computer hardware compatibility
(C) A tool provided free of charge to anyone wishing to test content conformance
(D) A developer resource requiring a high-priced annual subscription for access

**May/June 2025**

**22.** What does the acronym AICC stand for?
(A) Advanced International Content Committee
(B) Aviation Industry CBT Committee
(C) American Institute of Computer Courses
(D) Association of Interactive Content Creators

**Oct/Nov 2007**

**23.** How does e-Learning specifically benefit fast learners compared to conventional classroom training?
(A) Provision of supplementary printed textbooks and reading materials for review
(B) Mandating that high-performing students wait for the entire group to progress
(C) Granting immediate automated promotions to senior job designations within the company
(D) Allowing learners to complete training faster, thereby increasing individual productivity

**May/June 2014**

**24.** Which statement regarding LTI (Learning Tools Interoperability) is correct?
(A) A legacy standard that has been completely superseded by SCORM protocols
(B) A proprietary software tool developed and sold exclusively by Apple Inc.
(C) A security protocol that blocks third-party services from accessing the platform
(D) A standardized method for integrating rich learning applications with platforms

**Oct/Nov 2016**

**25.** Which domain of Bloom's Taxonomy represents growth in feelings or emotional areas?
(A) Cognitive
(B) Affective
(C) Psychomotor
(D) Somatic

**May/June 2018**

**26.** How are learning objects defined in the context of computer-based instruction?
(A) Large, monolithic instructional packages that remain undivided during deployment
(B) Tactile resources used exclusively within a conventional physical classroom setting
(C) Formal standardized examination papers utilized to evaluate and track learner progress
(D) Reusable elements of computer-based

Click Here to Buy book on Amazon

(B) A structure that allows students to grasp content with increasing depth
(C) A pedagogical focus exclusively on the development of physical skills
(D) Instruction delivered through the use of high-end virtual reality headsets

**Oct/Nov 2008**

**9.** Which statement accurately describes the function of IEEE LTSC?
(A) The exclusive development of training materials for the global aviation industry
(B) The provision of testable specifications that address industry best practices
(C) The focus on manufacturing standards for computer hardware components
(D) The management of learner registration and enrollment for online courses

**May/June 2024**

**10.** In which year did Benjamin Bloom propose the "Taxonomy of Educational Objectives"?
(A) 1945
(B) 1968
(C) 1956
(D) 1972

**Oct/Nov 2021**

**11.** Which statement regarding cmi5 is correct?
(A) A 2011 release that served as a technical precursor to the xAPI standard
(B) A project dissolved by the ADL and transferred back to the AICC organization
(C) A hardware specification defining the physical dimensions of an LMS server
(D) An xAPI companion specification for interoperability in traditional LMS settings

**May/June 2013**

**12.** What is Instructional Design?
(A) The aesthetic graphic design of interactive interfaces for mobile learning apps
(B) The physical architecture of modern virtual and brick-and-mortar classroom spaces
(C) The systematic translation of learning theory into instructional materials and plans
(D) The technical process of writing source code for an open-source management system

**Oct/Nov 2015**

**13.** What is the primary purpose of the "Web Safari" feature in a Virtual Classroom?
(A) A feature allowing instructors to take learners on a synchronized Web tour
(B) A tool permitting students to browse the internet anonymously during a session
(C) A security filter designed to block student access to unapproved websites
(D) An automated utility for downloading entire web pages for later offline reading

NODIA

**May/June 2020**

**14.** What is the characteristic of a "de facto" e-learning standard?
(A) A standard officially certified by an international accreditation body like the IEEE
(B) A regulation mandated by government agencies for all registered educational institutes
(C) A specification adopted and used because a critical mass chooses to do so
(D) A legacy technical specification that is no longer supported by modern software

**Oct/Nov 2005**

**15.** Which statement about mobile learning is correct regarding current trends?
(A) A trend currently viewed as the most overestimated in the e-learning industry
(B) A methodology that saw a complete halt in adoption during the global pandemic
(C) A learning approach utilized by universities but ignored by corporate entities
(D) A personalized learning method leveraged by nearly 4 billion smartphone users

**May/June 2017**

**16.** What is the primary function of a Learning Content Management System (LCMS)?
(A) To manage digital content from a central repository via creation, storage, and delivery
(B) To oversee user profiles and learning communities, including registration and approval workflows
(C) To establish standardized communication protocols between various instructional hardware devices
(D) To facilitate real-time high-definition video conferencing for large educational cohorts

**Oct/Nov 2024**

**17.** Which statement about the Experience API (Tin Can API) is correct?

is necessary to reduce costs because allowing expenses to scale linearly with data volume is not sustainable. By utilizing virtualization and efficient storage techniques, organizations can manage ten times the information without facing a corresponding ten-fold increase in costs.

**111.** (D) The increased productivity of business managers
Successful OLAP applications empower business managers to become more self-sufficient, allowing them to model complex problems and perform analysis without relying on IT for every change. This highlights the characteristic of increased productivity. By providing flexible tools for multidimensional analysis, organizations enable faster decision-making and more effective problem-solving, as users can explore historical data trends and perform what-if scenarios directly.

**112.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Both the assertion and the reason are true, and the reason correctly explains the assertion. Data warehouses remain relevant alongside data lakes because they serve different purposes. While data lakes store information in its raw form for flexible exploration, data warehouses provide a highly structured and transformed environment. This structure is essential for high-performance business intelligence, consistent reporting, and strategic decision-making.

**113.** (C) Assertion (A) is true, but Reason (R) is false.
The assertion that designing data warehouses is very different from designing traditional operational systems is true. These systems focus on broad, integrated business concepts rather than specific transactional tasks. However, the reason is false because data warehouse users typically do not know as much about their exact analytical needs as operational users do about their routine day-to-day requirements.

**114.** (B) Artificial Neural Network
An Artificial Neural Network is a system inspired by the biological information processing model of the human brain. It consists of interconnected processing nodes that receive information, process it, and pass states to other nodes. This structure allows the system to learn from data and identify complex patterns, making it highly effective for tasks such as detecting fraudulent insurance or banking claims.

**115.** (D) Data Granularity
The decision to subdivide a customer name into three distinct fields rather than storing it as a single string is a reflection of data granularity. This concept refers to the level of detail captured within the data model. Higher granularity provides more flexibility for analysis and reporting, allowing for more specific searches and categorization within the informational environment for decision-making.

**116.** (D) All (I), (II), (III), and (IV)
Data mining utilizes several algorithmic approaches to uncover insights. Associations identify items bought together in a single event. Classifications learn from pre-categorized past examples. Clustering discovers natural groupings based on common features in unclassified data. Forecasting uses statistical models to predict future behavior based on established relationships. Each of these techniques provides a unique way to analyze and interpret large organizational datasets.

**117.** (D) Associations
The retail chain is utilizing the associations approach in data mining to link the number of items purchased by a customer in a single visit. This technique identifies relationships between products that are frequently bought together. By understanding these natural buying patterns, businesses can optimize their shelf layouts, design more effective promotional strategies, and improve the overall shopping experience for their customers.

**118.** (B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
Both the assertion and the reason are true, but the reason does not correctly explain the assertion. A virtual data warehouse strategy minimizes data redundancy by avoiding the creation of a separate physical store. While it is also true that this approach can place a significant unplanned query load on operational systems, this load

Downloaded from www.pdf.tube

instruction delivered via the Internet

**Oct/Nov 2022**

**27.** Which statement regarding Virtual Classroom (VC) chat features is correct?
(A) A tool that fosters learner connection through immediate, clarifying responses
(B) A feature that creates social disorder similar to a physical classroom setting
(C) An interface where instructors are unable to answer queries in a timely manner
(D) A restricted communication tool intended only for the end of a training session

**May/June 2005**

**28.** What does the acronym Moodle stand for?
(A) Modular object-oriented dynamic learning environment
(B) Massive open online distance learning environment
(C) Multiple object-oriented digital learning execution
(D) Managed offline oriented dynamic learning engine

**Oct/Nov 2010**

**29.** Which of the following statements about updating e-learning material is correct?
(A) The manual distribution of physical update packages to every individual learner
(B) The inability to modify content once it has been published on the intranet
(C) Updating material without the costs of reprinting or distributing physical items
(D) The requirement for organizations to replace their entire LMS to update content

**May/June 2021**

**30.** Why is content packaging crucial in e-learning standards?
(A) Ensuring the visual layout adheres to established corporate branding guidelines
(B) Restricting learner access to the educational content outside of business hours
(C) Compressing high-resolution video files to optimize limited server storage space
(D) Enabling the transfer of courses and content between different learning systems

**Oct/Nov 2006**

**31.** Which of the following statements about Virtual Classroom tools is incorrect?
(A) Application sharing allows the instructor and students to share any Windows application
(B) Live voting allows the teacher to take feedback and has the discretion to make results public
(C) Web Safari automatically restricts learners from seeing the instructor's pointer during browsing
(D) Shared whiteboards allow the instructor to spend more time with students as course material is pre-prepared

**May/June 2019**

**32.** Which of the following is NOT a feature typically included in a Virtual Classroom?
(A) Voice conferencing
(B) Manual inventory management
(C) Breakout rooms
(D) Web Safari

NODIA

**Oct/Nov 2014**

**33.** Which of the following statements about e-learning standards is incorrect?
(A) Learner profile standards allow sharing of personal data, learning plans, and accessibility requirements
(B) Metadata content labeling must be inconsistent to prevent unauthorized discovery of learning objects
(C) Content packaging specifications enable the transfer of courses from one learning system to another
(D) Accredited standards ensure that the investment in intellectual capital could move from one system to the next

**May/June 2012**

**34.** What is the primary advantage of using "Shared whiteboards" in a Virtual Classroom?
(A) Restricting students from viewing any annotations made by the instructor
(B) The automatic grading of all multiple-choice questions in an assessment
(C) The complete elimination of the requirement for an active internet link
(D) Allowing saved markups on pre-prepared material to increase student time

**Oct/Nov 2025**

**35.** Which of the following is NOT a function typically managed by an LMS?
(A) Authoring and aggregating small units of

digital instructional content
(B) Creating course catalogues
(C) Registering learners and tracking approvals
(D) Scheduling classes

**May/June 2007**

**36.** What is the main function of a Learning Record Store (LRS)?
(A) To store experiential data statements in a format such as "actor verb object"
(B) To physically store printed certificates for learners
(C) To manage the payroll processing for instructional designers
(D) To broadcast live video streams to external social media platforms

**Oct/Nov 2018**

**37.** Which of the following statements about the advantages of e-learning is incorrect?
(A) The cost of developing and maintaining an e-learning application is always higher than an instructor-led training program
(B) It offers 24/7 accessibility to the workforce
(C) E-learning ensures that fast learners may complete their training sooner
(D) Unlimited colourful graphics and special effects can be delivered to direct attention

**May/June 2023**

**38.** Which of the following is NOT a phase in the ADDIE model?
(A) Analyze
(B) Design
(C) Evaluate
(D) Discover

**Oct/Nov 2009**

**39.** What is the most widely applied use of metadata in e-learning development?
(A) Encrypting data so that learners cannot view their individual test scores
(B) Compressing large video files to enable faster streaming over slow networks
(C) Automatically generating randomized multiple-choice questions for assessments
(D) Consistent labeling of content to support indexing, storage, and retrieval

**May/June 2016**

**40.** Which of the following statements about the impact of the pandemic on learning is incorrect?
(A) Online learning has become indispensable and grown at an exponential rate
(B) Almost every organization embraced learning and development technologies
(C) Organizations have been moving to video-based learning exponentially
(D) The learning and development (L&D) industry came to a complete and permanent grinding halt

**Oct/Nov 2020**

**41.** What is the correct chronological sequence of the phases in the ADDIE model?
(A) Analyze, Design, Develop, Implement, Evaluate
(B) Analyze, Develop, Design, Evaluate, Implement
(C) Design, Analyze, Implement, Develop, Evaluate
(D) Evaluate, Analyze, Design, Develop, Implement

**May/June 2022**

**42.** Which of the following statements about Experience API (Tin Can API) is incorrect?
(A) It solves many of the problems inherent with older versions of SCORM
(B) It allows software clients to read and write experiential data in the form of "statement" objects
(C) Experience API statements can only be stored within a Learning Management System (LMS)
(D) ADL is the steward of the Experience API

**Oct/Nov 2023**

**43.** Which of the following is NOT an aim of a Virtual Classroom in improving access and effectiveness of education?
(A) Promoting active learning rather than passive reception
(B) Increasing the physical travel requirements for hands-on labs
(C) Promoting group learning rather than a one-way show
(D) Decreasing time to earn a degree

**May/June 2011**

**44.** Which of the following is NOT one of the general categories into which most e-learning standards are organized?
(A) Metadata
(B) Content packaging

Click Here to Buy book on Amazon

(C) Learner profiles
(D) Graphic Interface Design

**Oct/Nov 2012**

**45.** What is the most significant advantage of Interactive Content as an emerging trend?
(A) The complete elimination of the professional role of the instructional designer
(B) Ensuring that learning content can only be viewed on desktop computer systems
(C) Using learning analytics to provide data for the Learning and Development path
(D) Forcing learners to consume all content at a fixed and unchangeable speed

**May/June 2015**

**46.** Which of the following statements about LCMS is incorrect?
(A) LCMS is a multi-user environment where developers can create and store digital learning content
(B) LCMS manages the process of scheduling classes, creating catalogues, and registering learners
(C) LCMS lets organizations take control of content by allowing multiple developers to share components
(D) LCMS provides authoring, sequencing, and aggregation tools

**Oct/Nov 2013**

**47.** In the context of instructional design, what is the best explanation for the term "readiness"?
(A) The speed at which a computer server boots up
(B) The experiences and contexts that make the student willing and able to learn
(C) The physical availability of classroom desks
(D) The completion of a prerequisite software installation

**May/June 2008**

**48.** Which of the following statements about Virtual Classroom Feedback is incorrect?
(A) Students can indicate yes/no polling and demonstrate applause responses
(B) Anonymous feedback is not possible in a Virtual Classroom, unlike a traditional classroom
(C) Students can utilize public or private text chat
(D) Anonymous feedback allows students to give their genuine views without hesitation

**Oct/Nov 2017**

**49.** Which of the following is NOT an emerging trend in e-learning post the Covid-19 pandemic?
(A) Floppy Disk Distribution
(B) Mobile Learning
(C) Gamification
(D) Video-based Learning

**May/June 2006**

**50.** Which of the following is NOT an objective of developing SCORM?
(A) Accessibility
(B) Durability
(C) Vulnerability
(D) Interoperability

**Oct/Nov 2008**

**51.** What is the fundamental idea behind learning objects?
(A) Large and unalterable textbook chapters presented in a digital format
(B) Physical instructional props used by trainers during live training sessions
(C) Standardized grading rubrics utilized by universities for formal examinations
(D) Small instructional units reusable across different learning contexts

**May/June 2024**

**52.** Which of the following statements about Bloom's Taxonomy is incorrect?
(A) The domains are also known as KSA (Knowledge, Skills, and Attitude)
(B) The Cognitive domain deals with mental skills
(C) It divides educational objectives into three domains
(D) The Psychomotor domain is concerned with growth in feelings or emotional areas

**Oct/Nov 2021**

**53.** Which of the following is NOT an advantage of creating an e-learning course?
(A) Cost savings compared to instructor-led training
(B) 24/7 accessibility to learning materials
(C) The ability to completely eliminate the need for physical office buildings
(D) The ability to update published content instantly

Downloaded from www.pdf.tube

traditional LMS environment entirely.

Which of the above statement(s) is/are correct?

(A) (I), (II), (III), and (V) only
(B) (I), (II), (III), and (IV) only
(C) (II), (III), (IV), and (V) only
(D) (I), (III), (IV), and (V) only

**May/June 2024**

**94.** Read the following scenario and answer the question that follows:

*A university replaces its physical lectures with a synchronous online environment. During a session, the professor takes the learners on a synchronized tour of a specific website, where students see the professor's pointer and automatically scroll when the professor scrolls. Which Virtual Classroom feature is the professor utilizing?*

(A) Application sharing
(B) Shared whiteboards
(C) Web Safari
(D) Live tests

**Oct/Nov 2021**

**95.** The following question consists of two statements — Assertion (A) and Reason (R). Answer this question selecting the appropriate option.

Assertion (A): A Virtual Classroom can radically reduce travel, facilities, and telecommunications costs.

Reason (R): A Virtual Classroom allows organizations to bring together large groups of people to interact and learn in a highly collaborative e-Learning environment.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2013**

**96.** Read the following scenario and answer the question that follows:

*A software company notices low employee engagement in mandatory cybersecurity training. The Learning & Development manager decides to revamp the training to showcase it as a "play thing" to allure learners and improve motivation for ROI. Which emerging e-learning trend is the manager adopting?*

(A) Video-based Learning
(B) Gamification
(C) Moodle deployment
(D) SCORM conformance testing

**Oct/Nov 2015**

**97.** Consider the following statements regarding the E-Learning environment:

I E-learning can deliver training via an organization's intranet or CD-ROM.
II E-learning cannot automatically track student answers using a learning management system.
III E-learning reduces the cost of developing and maintaining training applications.
IV An unlimited number of colourful graphics can be delivered in online courses.
V E-learning materials restrict access to a specific time zone.

Which of the above statement(s) is/are correct?

(A) (I), (III), and (IV) only
(B) (I), (II), and (V) only
(C) (II), (III), and (IV) only
(D) (I), (III), and (IV) only

**May/June 2020**

**98.** Read the following scenario and answer the question that follows:

*Once the institute implements the standard that uses the "actor verb object" format, they need a dedicated data store to save and query these experiential statements. What is the name of this required data store?*

(A) Learning Record Store (LRS)
(B) Central Object Repository
(C) Virtual Classroom Breakout Room
(D) Learning Management System (LMS)

**Oct/Nov 2005**

**99.** Read the following scenario and answer the question that follows:

*A corporate trainer is tasked with designing a new compliance curriculum. They begin by analyzing the learner characteristics and the task to be learned. Next, they develop the learning objectives and choose an instructional approach. Which established instructional design model is the trainer systematically following?*

(A) The SCORM Model
(B) The ADDIE Model

NODIA

# STUDYING FROM PDFs?

# THINK AGAIN.

If you are studying only from PDFs,
you are wasting valuable time.

Research shows that learning from

**PRINTED BOOKS** has up to

**4× HIGHER RETENTION**

than studying from screens.

**PRINT BOOK = BETTER MEMORY**

**PDF = LOWER RETENTION**

Those who study from **PRINTED BOOKS**
move **AHEAD.**

Others are left **BEHIND**
in competition.

In competitive exams,
being average is not enough.

## STAY ONE STEP AHEAD.

feedback allows students to give genuine views.
II In a traditional classroom, anonymous feedback is easily conducted through raising hands.
(A) Only (I) is correct
(B) Only (II) is correct
(C) Both (I) and (II) are correct
(D) Both (I) and (II) are incorrect

**Oct/Nov 2019**

**63.** Match the SCORM Objectives (List-I) with their correct meanings (List-II).
List I: (SCORM Objectives)
P. Accessibility
Q. Adaptability
R. Durability
S. Reusability
List II: (Meanings)
1. Ability to tailor instructions to individual and organizational needs
2. Extracting relevant modules from different courses to reassemble into a new one
3. Locating and accessing instructional components from one remote location to deliver to another
4. Adding new content to existing content without costly redesign
(A) P-3, Q-1, R-4, S-2
(B) P-1, Q-4, R-2, S-3
(C) P-4, Q-2, R-3, S-1
(D) P-2, Q-3, R-1, S-4

**May/June 2025**

**64.** Consider the following statements regarding emerging trends in e-learning:
I Mobile learning is considered underestimated despite about 4 billion people using smartphones.
II Gamification deters learners from engaging in training.
III Interactive content strategies utilize learning analytics to chalk out the L&D course.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

**Oct/Nov 2007**

**65.** Which of the following pairs is correctly matched regarding the ADDIE model?
(A) Design - Choose an instructional approach
(B) Analyze - Deliver or distribute the instructional materials
(C) Develop - Make sure the materials achieved the desired goals
(D) Implement - Analyze learner characteristics

**May/June 2014**

**66.** Consider the following statements regarding SCORM objectives:
I Accessibility allows finding content based on classification.
II Adaptability allows tailoring instructions without much effort.
III Affordability reduces time and costs in delivering content.
IV Durability requires content to be completely redesigned when technology evolves.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (III) only
(B) (I), (III), and (IV) only
(C) (II), (III), and (IV) only
(D) (I), (II), and (IV) only

**Oct/Nov 2016**

**67.** What is the correct chronological sequence of the following releases related to e-learning standards?
I Experience API v1.0 finalized
II Experience API released
III cmi5 released
(A) (I), (II), (III)
(B) (II), (I), (III)
(C) (III), (I), (II)
(D) (II), (III), (I)

**May/June 2018**

**68.** Read the following statements regarding learning systems and choose the correct option:
I LCMS focuses on course delivery and helps in getting the right content to the right people.
II LMS provides authoring, sequencing, and aggregation tools to structure content.
(A) Only (I) is correct
(B) Only (II) is correct
(C) Both (I) and (II) are correct
(D) Both (I) and (II) are incorrect

**Oct/Nov 2022**

**69.** Consider the following statements regarding the Moodle learning management system:

Click Here to Buy book on Amazon

May/June 2013

**54.** What is the best description of an instructional system?
(A) A software algorithm that grades essays automatically
(B) A hardware server dedicated to hosting video content
(C) An arrangement of resources and procedures to promote learning
(D) A regulatory body that issues educational degrees

Oct/Nov 2015

**55.** Which of the following is NOT a domain in Bloom's Taxonomy of Educational Objectives?
(A) Intuitive
(B) Cognitive
(C) Affective
(D) Psychomotor

May/June 2020

**56.** Which of the following statements about AICC is incorrect?
(A) It exclusively develops standards that are only applicable to and used by the aviation industry
(B) It stands for Aviation Industry CBT Committee
(C) It publishes the Computer-Managed Instruction (CMI) guidelines
(D) Its membership decided to dissolve the organization and transferred cmi5 to ADL

Oct/Nov 2005

**57.** What is the chief benefit of adopting SCORM standardization?
(A) Ensuring content reusability across courses and LMSs without constraints
(B) Locking educational content to a single, proprietary management system
(C) The automatic conversion of text documents into virtual reality simulations
(D) Requiring instructional developers to completely redesign content annually

May/June 2017

**58.** Which of the following statements about Moodle is incorrect?
(A) It is a proprietary, closed-source learning management system
(B) It is written in PHP and distributed under the GNU General Public License
(C) It uses the External Tool activity to act as an 'LTI consumer' as standard
(D) It is developed on pedagogical principles and used for blended learning

Oct/Nov 2024

**59.** What is the primary goal of e-learning standards?
(A) To significantly increase the overhead costs of developing online training
(B) To mandate a specific visual branding style for all corporate e-learning
(C) To provide standardized data structures and protocols for cross-system work
(D) To restrict the sharing of instructional content across disparate platforms

May/June 2010

**60.** Which of the following is NOT an accrediting organization recognized for developing e-learning standards?
(A) AICC
(B) HTML
(C) IEEE
(D) ADL

Oct/Nov 2011

**61.** Match the emerging trends (List-I) with their characteristics (List-II).
List I: (Emerging Trends)
P. Mobile Learning
Q. Video-based Learning
R. Gamification
S. Interactive Content
List II: (Characteristics)
1. Allures learners by showcasing training as a 'play thing'
2. Uses learning analytics to chalk out the L&D course
3. Paves the way for personalized learning leveraging the widespread use of smartphones
4. Gained immense prominence exponentially after the Covid-19 breakout
(A) P-1, Q-2, R-3, S-4
(B) P-4, Q-1, R-2, S-3
(C) P-3, Q-4, R-1, S-2
(D) P-2, Q-3, R-4, S-1

May/June 2009

**62.** Read the following statements regarding feedback in different classroom environments and choose the correct option:
I In a Virtual Classroom, anonymous

NODIA

organization.

Which of the above statement(s) is/are correct?

(A) (I), (II), and (III) only
(B) (I), (III), and (IV) only
(C) (II), (III), and (IV) only
(D) (I), (II), (III), and (IV)

**May/June 2012**

**76.** Match the following standard organizations (List-I) with their descriptions (List-II).

List I: (Standard Organizations)

P. AICC
Q. IEEE LTSC
R. IMS
S. ADL

List II: (Descriptions)

1. A U.S. government-sponsored organization that developed SCORM
2. An international group creating CBT-related guidelines originally for the aviation industry
3. Focuses mostly on metadata for tagging learning objects and content packaging
4. Provides specifications like the Learning Object Metadata (LOM) specification

(A) P-1, Q-2, R-4, S-3
(B) P-3, Q-1, R-2, S-4
(C) P-4, Q-3, R-1, S-2
(D) P-2, Q-4, R-3, S-1

**Oct/Nov 2025**

**77.** Consider the following statements regarding Bloom's Taxonomy:

I It was proposed by Benjamin Bloom in 1956.
II The affective domain is associated with manual or physical skills.
III The taxonomy of learning behaviours can be thought of as the goals of the training process.

Which of the above statement(s) is/are correct?

(A) (I) and (II) only
(B) (I) and (III) only
(C) (II) and (III) only
(D) (I), (II), and (III)

**May/June 2007**

**78.** Match the system or standard (List-I) with its core function (List-II).

List I: (System/Standard)

P. LMS
Q. LCMS
R. LTI
S. LRS

List II: (Core Functions)

1. Stores experiential data statements
2. Integrates rich learning applications with educational platforms
3. Manages users, scheduling, and registration
4. Manages the creation, storage, and reuse of digital content

(A) P-4, Q-3, R-1, S-2
(B) P-1, Q-2, R-3, S-4
(C) P-2, Q-1, R-4, S-3
(D) P-3, Q-4, R-2, S-1

**Oct/Nov 2018**

**79.** Read the following statements regarding the impact of the Covid-19 pandemic on e-learning and choose the correct option:

I The Covid-19 pandemic caused the e-learning industry to come to a grinding halt along with other businesses.
II Video-based learning gained immense prominence after the Covid-19 breakout.

(A) Only (I) is correct
(B) Only (II) is correct
(C) Both (I) and (II) are correct
(D) Both (I) and (II) are incorrect

**May/June 2023**

**80.** Which of the following pairs is incorrectly matched regarding SCORM objectives?

(A) Accessibility - Delivering components from one remote location to other locations
(B) Interoperability - Running courses on different learning and content management systems
(C) Reusability - Extracting relevant modules to reassemble into a new course
(D) Durability - Reducing the time and costs involved in delivering instructional content

**Oct/Nov 2009**

**81.** Consider the following statements regarding the ADDIE model of instructional design:

I Analyze involves evaluating learner characteristics.
II Design involves choosing an instructional approach.
III Develop involves creating training materials.
IV Evaluate is performed only once and marks the permanent end of the process.

Which of the above statement(s) is/are correct?

(A) (I), (II), and (III) only

Downloaded from www.pdf.tube

(B) (I), (II), and (IV) only
(C) (II), (III), and (IV) only
(D) (I), (III), and (IV) only

**May/June 2016**

**82.** Match the Virtual Classroom features (List-I) with their descriptions (List-II).
List I: (Virtual Classroom Features)
P. Voice conferencing
Q. Shared whiteboards
R. Web Safari
S. Breakout rooms
List II: (Descriptions)
1. Leading a live, synchronized web browsing session
2. Dividing the main session for team or individual lab exercises
3. Fully integrated, multi-way audio that helps identify who is speaking
4. Interactive markup that can be saved for later review
(A) P-3, Q-4, R-1, S-2
(B) P-4, Q-1, R-2, S-3
(C) P-1, Q-2, R-3, S-4
(D) P-2, Q-3, R-4, S-1

**Oct/Nov 2020**

**83.** Match the acronyms (List-I) to their associated concepts (List-II).
List I: (Acronyms)
P. CAM
Q. RTE
R. KSA
S. xAPI
List II: (Concepts)
1. Run-Time Environment
2. Tin Can API
3. Knowledge, Skills, and Attitude
4. Content Aggregation Model
(A) P-1, Q-2, R-4, S-3
(B) P-3, Q-4, R-2, S-1
(C) P-2, Q-3, R-1, S-4
(D) P-4, Q-1, R-3, S-2

**May/June 2022**

**84.** Consider the following statements regarding e-learning standard categories:
I Metadata standards support the indexing and discovery of learning objects.
II Content packaging specifies rules for delivering content to a learner.
III Learner profiles allow systems to communicate data such as scores or completion status.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

**Oct/Nov 2023**

**85.** Read the following statements regarding the Experience API and choose the correct option:
I Experience API (Tin Can API) statements are stored in a data store called a Learning Record Store (LRS).
II An LRS can exist on its own or within a Learning Management System (LMS).
(A) Only (I) is correct
(B) Only (II) is correct
(C) Both (I) and (II) are correct
(D) Both (I) and (II) are incorrect

**May/June 2011**

**86.** Match Bloom's Taxonomy Domains (List-I) with their corresponding elements (List-II).
List I: (Bloom's Taxonomy Domains)
P. Cognitive
Q. Affective
R. Psychomotor
S. KSA equivalent of Affective
List II: (Elements)
1. Skills
2. Attitude
3. Knowledge
4. Growth in feelings or emotional areas
(A) P-1, Q-2, R-4, S-3
(B) P-3, Q-4, R-1, S-2
(C) P-4, Q-1, R-3, S-2
(D) P-2, Q-3, R-1, S-4

**Oct/Nov 2012**

**87.** Consider the following statements regarding LMS and LCMS functionalities:
I LMS manages users and communities (registration, assignment, approvals).
II LCMS focuses on course delivery.
III LMS provides authoring, sequencing, and aggregation tools.
IV LCMS renders content and tracks learners' bookmarks to pass back to LMS.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (IV) only
(B) (I), (II), and (III) only

NODIA

(C) (II), (III), and (IV) only
(D) (I), (III), and (IV) only

**May/June 2015**

**88.** Match the Virtual Classroom tools (List-I) with their specific advantages over physical classrooms (List-II).

List I: (Virtual Classroom Tools)
P. Audience control tools
Q. Feedback
R. Live tests
S. Live presentation tools

List II: (Advantages)
1. Enables anonymous responses, preventing students from hesitating to give genuine views
2. Includes Flash, DHTML, JavaScript, and animated GIFs
3. The teacher can refuse to hand over the mic to a mischievous student
4. Assessment is tracked and reported online with custom reports easily generated

(A) P-1, Q-3, R-2, S-4
(B) P-3, Q-1, R-4, S-2
(C) P-4, Q-2, R-1, S-3
(D) P-2, Q-4, R-3, S-1

**Oct/Nov 2013**

**89.** Consider the following statements regarding the advantages of e-learning:
I It ensures fast learners complete their training sooner.
II It limits staff training by imposing strict constraints on resources.
III It offers 24/7 accessibility.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

**May/June 2008**

**90.** Which of the following pairs is incorrectly matched regarding e-learning standards organizations?
(A) IMS - Primarily focuses on developing web browser software
(B) AICC - Computer-Managed Instruction (CMI) guidelines
(C) IEEE LTSC - Learning Object Metadata (LOM) specification
(D) ADL - Shareable Content Object Reference Model (SCORM)

**Oct/Nov 2017**

**91.** The following question consists of two statements — Assertion (A) and Reason (R). Answer this question selecting the appropriate option.
Assertion (A): Unlike conventional learning methods, e-learning ensures that fast learners may complete their training sooner.
Reason (R): E-learning materials may be made accessible to the workforce throughout the day on a 24/7 basis.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2006**

**92.** Read the following scenario and answer the question that follows:
*An aviation training institute has developed extensive e-learning content. To protect their intellectual capital, they want to ensure their courses can be moved seamlessly to a different delivery platform in the future without losing data or functionality, avoiding proprietary constraints. Which model specifically addresses this reusability across courses and management systems without proprietary constraints?*
(A) Virtual Classroom (VC) Voice Conferencing
(B) The Cognitive domain of Bloom's Taxonomy
(C) SCORM (Shareable Content Object Reference Model)
(D) HTML (HyperText Markup Language)

**Oct/Nov 2008**

**93.** Consider the following statements about the Experience API and associated protocols:
I The Experience API was finalized to version 1.0 in April 2013.
II It records statements in an "actor verb object" format.
III Experience API statements are stored in a Learning Record Store (LRS).
IV cmi5 is a companion specification to xAPI released in 2016.
V cmi5 was developed to eliminate the

Click Here to Buy book on Amazon

I It is a proprietary, closed-source learning management system.
II It is written in PHP and distributed under the GNU General Public License.
III It allows extending and tailoring learning environments using community sourced plugins.

Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

**May/June 2005**

**70.** Match the e-learning standard categories (List-I) with their focus areas (List-II).
List I: (Standard Categories)
P. Metadata
Q. Content packaging
R. Learner profiles
S. Accrediting organizations
List II: (Focus Areas)
1. Sharing personal data, certifications, and assessment scores
2. Labelling to support indexing, discovery, and retrieval
3. AICC, IEEE, IMS, and ADL
4. Enabling transfer of courses from one learning system to another
(A) P-1, Q-3, R-2, S-4
(B) P-4, Q-1, R-3, S-2
(C) P-2, Q-4, R-1, S-3
(D) P-3, Q-2, R-4, S-1

**Oct/Nov 2010**

**71.** Consider the following statements regarding Virtual Classroom (VC) features:
I Voice conferencing is fully integrated and full duplex.
II Shared whiteboards allow markup on pre-prepared materials to be saved.
III Web Safari allows the instructor to lead a live web browsing session.
IV Breakout rooms permit the instructor to take control of applications within the smaller sessions.

Which of the above statement(s) is/are correct?
(A) (I), (II), and (III) only
(B) (I), (III), and (IV) only
(C) (II), (III), and (IV) only
(D) (I), (II), (III), and (IV)

**May/June 2021**

**72.** Match the ADDIE model phases (List-I) with their primary activities (List-II).
List I: (ADDIE Phases)
P. Analyze
Q. Design
R. Develop
S. Evaluate
List II: (Activities)
1. Make sure the materials achieved the desired goals
2. Create instructional or training materials
3. Develop learning objectives, choose an instructional approach
4. Assess learner characteristics, task to be learned
(A) P-1, Q-4, R-3, S-2
(B) P-4, Q-3, R-2, S-1
(C) P-3, Q-2, R-1, S-4
(D) P-2, Q-1, R-4, S-3

**Oct/Nov 2006**

**73.** Read the following statements regarding instructional design and choose the correct option:
I Instructional design is usually the final stage of systematic instruction.
II The ADDIE model's five phases end permanently once the training program is implemented.
(A) Only (I) is correct
(B) Only (II) is correct
(C) Both (I) and (II) are correct
(D) Both (I) and (II) are incorrect

**May/June 2019**

**74.** Which of the following pairs is correctly matched regarding Bloom's Taxonomy domains and KSA?
(A) Cognitive - Attitude
(B) Affective - Skills
(C) Cognitive - Knowledge
(D) Psychomotor - Knowledge

**Oct/Nov 2014**

**75.** Consider the following statements regarding e-learning standard organizations:
I AICC creates CBT-related guidelines.
II IEEE LTSC developed the SCORM model.
III IMS focuses mostly on metadata for tagging learning objects.
IV ADL is a U.S. government-sponsored

NODIA

(C) The LTI Model
(D) The Experience API Model

**May/June 2017**

**100.** The following question consists of two statements — Assertion (A) and Reason (R). Answer this question selecting the appropriate option.
Assertion (A): SCORM requires that courses can run on different learning and content management systems.
Reason (R): The SCORM objective of Interoperability means instructional components developed in one location can be used or combined with another set of tools or platform in another location.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2024**

**101.** Read the following scenario and answer the question that follows:
*The company also noted that after the Covid-19 breakout, one specific method topped the list of learning means and methods, gaining immense prominence exponentially. Which method is this?*
(A) Video-based Learning
(B) Mobile Learning
(C) Synchronous text-based chat
(D) Printed correspondence courses

**May/June 2010**

**102.** Consider the following statements regarding emerging trends and the impact of the Covid-19 pandemic on e-learning:
I The pandemic smashed earlier estimations of e-learning trends.
II Online learning has become indispensable and grown at an exponential rate.
III Mobile learning paves the way for a personalized learning opportunity.
IV Video-based learning has lost prominence due to bandwidth constraints post-Covid.
V Gamification motivates L&D managers to get more out of training.
Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (V) only
(B) (I), (II), (III), and (IV) only
(C) (II), (III), (IV), and (V) only
(D) (I), (III), (IV), and (V) only

**Oct/Nov 2011**

**103.** Read the following scenario and answer the question that follows:
*In the system chosen for authoring, the designers create small digital instructional components that can be reused in multiple contexts and delivered over the intranet. What is the specific technical term used to describe these small, reusable digital instructional components?*
(A) Metadata profiles
(B) Learning Objects
(C) ADDIE phases
(D) Content packages

**May/June 2009**

**104.** The following question consists of two statements — Assertion (A) and Reason (R). Answer this question selecting the appropriate option.
Assertion (A): Anonymous feedback allows students to give their genuine views without hesitation in a Virtual Classroom.
Reason (R): The traditional physical classroom also allows the exact same anonymous feedback process to occur seamlessly.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2019**

**105.** Read the following scenario and answer the question that follows:
*The professor uses pre-prepared course material and wishes to annotate it live. These multi-user interactive markups need to be saved for later review by the students. Which Virtual Classroom feature allows for this specific functionality?*
(A) Video conferencing
(B) Web Safari
(C) Shared whiteboards
(D) Application sharing

NODIA

May/June 2025

**106.** Consider the following statements regarding e-learning standards and specifications:

I HTML is an example of a de facto standard based on common use.

II IEEE certification grants a specification the status of a de jure standard.

III SCORM combines elements of IEEE, AICC, and IMS specifications.

IV LTI uses the External Tool activity to act as an 'LTI provider' in Moodle.

V The SCORM Conformance Test Suite must be purchased by developers.

Which of the above statement(s) is/are correct?

(A) (I), (II), and (III) only
(B) (I), (III), and (V) only
(C) (II), (III), and (IV) only
(D) (I), (II), and (III), and (IV) only

Oct/Nov 2007

**107.** Read the following scenario and answer the question that follows:

*During the final evaluation phase, the trainer uses a taxonomy to determine if the learners have acquired new manual or physical skills necessary for operating a new machine. Which domain of Bloom's Taxonomy encompasses these manual or physical skills?*

(A) Psychomotor
(B) Cognitive
(C) Affective
(D) Knowledge

May/June 2014

**108.** The following question consists of two statements — Assertion (A) and Reason (R). Answer this question selecting the appropriate option.

Assertion (A): HTML is considered a de facto standard in web development.

Reason (R): HTML received its stamp of approval directly from an accrediting body such as IEEE.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Oct/Nov 2016

**109.** Read the following scenario and answer the question that follows:

*The same aviation institute now wants to track experiential data outside the traditional web-browser environment, such as a simulator exercise. They need a standard that allows software clients to read and write experiential data in a flexible "actor verb object" format. Which standard should they implement?*

(A) SCORM version 1.2
(B) IEEE LTSC LOM specification
(C) IMS Global Consortium packaging
(D) Experience API (Tin Can API / xAPI)

May/June 2018

**110.** The following question consists of two statements — Assertion (A) and Reason (R). Answer this question selecting the appropriate option.

Assertion (A): SCORM standardization allows instructional designers to focus on creating better e-learning content, acting as a force multiplier.

Reason (R): SCORM standardization increases student retention and comprehension while realizing a concurrent decrease in cost and time.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Oct/Nov 2022

**111.** Read the following scenario and answer the question that follows:

*To further refine the training program, the manager decides to use learning analytics to provide the necessary data to chalk out the course of their L&D. This strategy is a significant part of which emerging e-learning trend?*

(A) Mobile Learning
(B) Virtual Classroom Audience Control
(C) Content Packaging
(D) Interactive Content

May/June 2005

**112.** The following question consists of two statements — Assertion (A) and Reason (R).

Downloaded from www.pdf.tube

Answer this question selecting the appropriate option.
Assertion (A): E-learning often provides significant cost savings for corporations and schools.
Reason (R): Learning material can be updated without the expense of reprinting a book, storing inventory, or manually distributing an update.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2010**

**113.** The following question consists of two statements — Assertion (A) and Reason (R). Answer this question selecting the appropriate option.
Assertion (A): Bloom's Taxonomy divides educational objectives into Cognitive, Affective, and Psychomotor domains.
Reason (R): The Affective domain is primarily concerned with manual or physical skills.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2021**

**114.** Read the following scenario and answer the question that follows:
*As the trainer progresses through the ADDIE model, they reach the phase where they physically create the instructional or training materials. Which phase of the ADDIE model does this represent?*
(A) Analyze
(B) Develop
(C) Design
(D) Implement

**Oct/Nov 2006**

**115.** Read the following scenario and answer the question that follows:
*Following the implementation of the system to manage users, the bank's instructional designers request a tool that allows them to author, sequence, and aggregate digital content. They want multiple subject matter experts to share small instructional components to build courses. Which system is designed to provide this functionality?*
(A) Learning Management System (LMS)
(B) Computer-Managed Instruction (CMI)
(C) Advanced Distributed Learning (ADL)
(D) Learning Content Management System (LCMS)

**May/June 2019**

**116.** Consider the following statements regarding Virtual Classroom capabilities:
I It promotes active learning rather than passive reception.
II It supports live ad-hoc learning discussions and study sessions.
III Its adaptive video bandwidth feature works over connections as low as 480 kbps.
IV It prevents sharing of Windows applications to maintain security.
V It allows audience control tools, where the teacher may refuse to hand over the mic.
Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (V) only
(B) (I), (II), (IV), and (V) only
(C) (II), (III), (IV), and (V) only
(D) (I), (III), (IV), and (V) only

NODIA

**Oct/Nov 2014**

**117.** Read the following scenario and answer the question that follows:
*Later in the same online session, the professor wants the students to collaborate in small groups on a lab exercise without distracting the rest of the class. The professor wants to be able to "look over the shoulder" of these smaller groups. Which feature should the professor use to split the main session?*
(A) Voice conferencing
(B) Audience control tools
(C) Live voting
(D) Breakout rooms

**May/June 2012**

**118.** The following question consists of two statements — Assertion (A) and Reason (R). Answer this question selecting the appropriate option.

**33.** (B) Metadata content labeling must be inconsistent to prevent unauthorized discovery of learning objects
Standards for metadata in e-learning actually require highly consistent labeling to facilitate the easy discovery and retrieval of learning objects. Inconsistency would hinder the ability of systems to index and organize content effectively. The goal of these standards is to support the sharing and reuse of educational components by ensuring they are described using a uniform and recognizable framework.

**34.** (D) Allowing saved markups on pre-prepared material to increase student time
Shared whiteboards in virtual classrooms significantly enhance instruction by allowing teachers to use pre-prepared materials. Instructors can annotate these materials live with markups that can be saved for later review. This efficiency allows the teacher to spend more time interacting with students rather than manually drawing content, thereby maximizing the instructional value of each synchronous and collaborative learning session.

**35.** (A) Authoring and aggregating small units of digital instructional content
A Learning Management System primarily handles the administrative side of education, such as class scheduling, course cataloging, and student tracking. The specific tasks of authoring and aggregating small units of digital instructional content are typically the domain of a Learning Content Management System. While some platforms offer both capabilities, these functions are distinct in traditional digital learning architecture and classifications.

**36.** (A) To store experiential data statements in a format such as "actor verb object"
A Learning Record Store is a data storage system designed specifically to house experiential learning records. It utilizes the Experience API format to capture a wide range of learning activities as statements involving an actor, a verb, and an object. Unlike traditional systems, an LRS can record learning that happens anywhere, including mobile apps, simulators, or various offline environments.

**37.** (A) The cost of developing and maintaining an e-learning application is always higher than an instructor-led training program
While initial development of e-learning content can require a significant investment, it often results in long-term cost savings compared to traditional instructor-led training. E-learning eliminates recurring expenses such as instructor travel, facility rentals, and physical material distribution. Therefore, stating that e-learning is always more expensive is incorrect, as it scales more efficiently for large and geographically dispersed workforces.

**38.** (D) Discover
The ADDIE model is a foundational instructional design framework consisting of five specific phases: Analysis, Design, Development, Implementation, and Evaluation. While "Discover" may be used in other business or design methodologies, it is not one of the standardized steps in this particular instructional system design model. Each phase in ADDIE has a distinct role in ensuring that training is effective.

**39.** (D) Consistent labeling of content to support indexing, storage, and retrieval
In the development of e-learning, metadata is most commonly used to provide consistent labeling for digital assets. This descriptive information allows learning objects to be easily indexed, stored, and retrieved within a management system. By using standardized metadata fields, organizations ensure that their instructional materials are searchable and reusable across different courses and platforms, significantly improving content management efficiency.

**40.** (D) The learning and development (L&D) industry came to a complete and permanent grinding halt
Contrary to coming to a halt, the learning and development industry experienced unprecedented growth and transformation during the pandemic. Organizations rapidly adopted digital technologies to ensure continuity of education and training. While many physical events were canceled, the shift toward online learning, virtual classrooms, and video-based instruction became indispensable, leading to an exponential increase in the usage of digital platforms.

Click Here to Buy book on Amazon

(B) Affordability
(C) Reusability
(D) Accessibility

NODIA

**Oct/Nov 2020**

**125.** Read the following scenario and answer the question that follows:
*A multinational corporation integrates rich learning applications provided through third-party services with their educational platforms. They require a standard way to achieve this integration acting as a consumer and provider. Which standard is specifically designed for this type of integration?*
(A) AICC Computer-Managed Instruction
(B) LTI (Learning Tools Interoperability)
(C) SCORM Content Aggregation Model
(D) Bloom's Taxonomy

www.nodia.in

Assertion (A): Instructional Design is the systematic process of translating general learning principles into instructional materials.
Reason (R): Instructional Design helps ensure the quality of instruction by analyzing learning needs and goals to develop a delivery system to meet those needs.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2025**

**119.** Read the following scenario and answer the question that follows:
*Once the institute implements the standard that uses the "actor verb object" format, they need a dedicated data store to save and query these experiential statements. What is the name of this required data store?*
(A) Learning Record Store (LRS)
(B) Central Object Repository
(C) Virtual Classroom Breakout Room
(D) Learning Management System (LMS)

**May/June 2007**

**120.** The following question consists of two statements — Assertion (A) and Reason (R). Answer this question selecting the appropriate option.
Assertion (A): Mobile Learning is considered an underestimated and underexplored e-learning trend by corporates.
Reason (R): Out of a nearly 8 billion global population, about 4 billion people use smartphones.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2018**

**121.** Read the following scenario and answer the question that follows:
*The client decides to host the newly purchased module on a free and open-source software learning management system written in PHP, developed on pedagogical principles, and distributed under the GNU General Public License. Which platform is the client using?*
(A) LCMS
(B) SCORM Test Suite
(C) Learning Record Store (LRS)
(D) Moodle

**May/June 2023**

**122.** Read the following scenario and answer the question that follows:
*An independent content developer creates a module on financial literacy. They want to ensure that if a client upgrades their technology infrastructure, the new content can be added to existing content without any costly redesign, reconfiguration, or recoding. Which specific objective of SCORM is the developer aiming to meet?*
(A) Accessibility
(B) Adaptability
(C) Durability
(D) Interoperability

**Oct/Nov 2009**

**123.** Read the following scenario and answer the question that follows:
*The corporation eventually decides they need interoperability in their traditional LMS environment using xAPI as the underlying communication protocol and data format. They adopt a companion specification to xAPI released in 2016. What is the name of this companion specification?*
(A) Tin Can API v1.0
(B) SCORM 1.2
(C) cmi5
(D) IEEE LOM

**May/June 2016**

**124.** Read the following scenario and answer the question that follows:
*The developer also wants to guarantee that the client can use the module on any platform, meaning the instructional components developed in their location can run combined with another set of tools in another location. Which SCORM objective does this refer to?*
(A) Interoperability

Downloaded from www.pdf.tube

allowing students to gain a more sophisticated understanding and greater depth of the subject matter. This approach ensures that learners reinforce foundational skills before tackling more complex and specialized applications of the content.

9. (B) The provision of testable specifications that address industry best practices
The IEEE Learning Technology Standards Committee is dedicated to developing technical standards for learning technology. It provides testable specifications that reflect industry best practices, ensuring interoperability between different educational systems. By establishing these frameworks, the committee helps organizations create and deploy learning objects that can be consistently recognized and utilized across various software platforms and institutional training environments globally.

10. (C) 1956
Benjamin Bloom proposed the "Taxonomy of Educational Objectives" in 1956. This influential framework was designed to classify educational goals and learning behaviors into hierarchical levels. By providing a common language for educators, it facilitates the design of curricula and assessments that target different levels of cognitive complexity, ranging from basic recall and understanding to advanced evaluation and synthesis.

11. (D) An xAPI companion specification for interoperability in traditional LMS settings
The cmi5 specification serves as a critical bridge between the flexible xAPI standard and the structured environment of traditional Learning Management Systems. Released in 2016, it provides a set of rules for how xAPI statements should be recorded and communicated within an LMS. This ensures interoperability while maintaining the robust and detailed tracking capabilities required for modern digital learning.

12. (C) The systematic translation of learning theory into instructional materials and plans
Instructional design is a systematic process focused on creating effective educational experiences. It involves the careful translation of psychological and educational theories into practical materials and structured plans. By analyzing learner needs and defining clear objectives, designers ensure that the resulting instructional content is engaging, efficient, and successfully facilitates the acquisition of knowledge or the development of specific skills.

NODIA

13. (A) A feature allowing instructors to take learners on a synchronized Web tour
The Web Safari feature enhances collaborative learning in virtual environments by allowing instructors to lead students on synchronized web tours. During these sessions, the instructor's browser activities, such as scrolling and clicking, are mirrored on the students' screens. This tool enables real-time exploration of online resources, ensuring all participants remain focused on the same web content simultaneously during instruction.

14. (C) A specification adopted and used because a critical mass chooses to do so
A de facto standard emerges in the marketplace through widespread adoption and usage rather than through official certification by a formal governing body. When a critical mass of developers and organizations chooses a particular specification, it becomes the industry norm. This type of standard relies on its practical utility and broad acceptance to achieve dominance within the technological ecosystem over time.

15. (D) A personalized learning method leveraged by nearly 4 billion smartphone users
Mobile learning has transformed education by providing personalized opportunities for millions of users worldwide. With nearly four billion people utilizing smartphones, this methodology leverages ubiquity to deliver training at the point of need. It allows learners to engage with content anytime and anywhere, making it one of the most significant and rapidly growing trends in modern digital education today.

16. (A) To manage digital content from a central repository via creation, storage, and delivery
A Learning Content Management System is primarily designed to handle the lifecycle of digital instructional materials. It provides a central repository where content can be created, stored, and reused across various courses. By focusing on the granular management of learning objects, it enables developers to efficiently organize,

# ANSWERS

1. (D) 2013
The Experience API, also known as Tin Can API, reached its finalized 1.0 version in April 2013. This standard allows for tracking learning experiences across various platforms and devices. It was developed by the Advanced Distributed Learning Initiative to overcome limitations found in earlier SCORM versions by providing a more flexible tracking mechanism for modern digital education.

2. (C) The application need not be installed on every student's PC, unlike a traditional lab setting
Virtual classrooms provide a significant advantage regarding software accessibility through application sharing. Unlike traditional computer labs where every machine requires individual installations and licenses, virtual settings allow instructors to share an active software view. This eliminates the technical burden and financial cost associated with maintaining software across multiple physical workstations for every student participating in the training session.

3. (C) Learning processes including class scheduling, catalog creation, and learner registration
A Learning Management System serves as the administrative backbone for educational activities. It focuses on organizational tasks such as maintaining course catalogs, managing student registrations, and scheduling various classes. By automating these processes, the system streamlines the delivery and tracking of training while providing a centralized hub for learners to access their assigned programs and monitor their individual progress.

4. (C) A 1956 model dividing objectives into Cognitive, Affective, and Psychomotor
Developed in 1956 by Benjamin Bloom and his colleagues, this framework categorizes educational goals into three primary domains. These include the cognitive domain for mental skills, the affective domain for emotional growth, and the psychomotor domain for physical or manual skills. It provides a structured approach for educators to design assessments and learning objectives effectively across different educational levels.

5. (B) It allows the data to be passed back to the LMS for reporting purposes
The interaction between an LCMS and an LMS is crucial for comprehensive learner tracking. While the LCMS manages content rendering and captures granular data like bookmarks or scores, it ultimately passes this information back to the LMS. This integration ensures that administrative records remain accurate, allowing organizations to generate detailed reports on learner progress and performance across various courses.

6. (B) A cyclical loop where the five phases are continually and regularly repeated
The ADDIE model is characterized by its iterative nature rather than being a strictly linear process. It consists of five distinct phases: analysis, design, development, implementation, and evaluation. These stages form a cyclical loop, allowing instructional designers to continually refine and improve training programs based on feedback and results obtained during the various stages of content development and delivery.

7. (B) Learning and teaching delivered through electronic media, particularly the Internet
E-learning represents a modern educational methodology where instruction is facilitated through electronic technologies. This approach primarily utilizes the Internet and intranets to deliver content, enabling flexible learning environments. It encompasses various digital formats, including multimedia presentations and interactive modules, allowing students to access training materials and interact with instructors or peers from remote locations around the world seamlessly.

8. (B) A structure that allows students to grasp content with increasing depth
Spiral organization in instructional design refers to a curriculum structure where key concepts are revisited multiple times throughout a course. Each revisit builds upon previous knowledge,

Click Here to Buy book on Amazon

**25.** (B) Affective
The affective domain in Bloom's Taxonomy specifically addresses growth in emotional areas, including feelings, values, appreciation, enthusiasms, and attitudes. It is one of the three foundational categories of educational objectives. This domain focuses on the internal processes of learners as they develop personal perspectives and emotional responses to the information or skills they are acquiring during their education.

**26.** (D) Reusable elements of computer-based instruction delivered via the Internet
In computer-based instruction, learning objects are defined as small, reusable units of digital content. These elements are designed to be self-contained and modular, allowing them to be combined in various ways to create different courses or lessons. Typically delivered via the Internet, they support flexible and efficient instructional design by enabling the reuse of high-quality components across multiple platforms.

**27.** (A) A tool that fosters learner connection through immediate, clarifying responses
Chat features in a virtual classroom serve as a vital communication bridge between instructors and students. They foster a sense of connection by allowing for immediate interaction and clarifying questions without interrupting the main presentation. This tool supports active participation and real-time feedback, ensuring that learners can quickly resolve doubts and stay engaged with the ongoing synchronous educational activities.

**28.** (A) Modular object-oriented dynamic learning environment
Moodle stands for Modular Object-Oriented Dynamic Learning Environment. It is a widely used, open-source Learning Management System designed to provide educators, administrators, and learners with a robust, secure, and integrated platform. Built on pedagogical principles, it allows for the creation of personalized learning environments using a modular structure that can be easily expanded with various community-developed plugins.

**29.** (C) Updating material without the costs of reprinting or distributing physical items
One of the primary economic advantages of e-learning is the ease and speed of content updates. Organizations can modify digital materials instantly within their learning management systems without incurring expenses for reprinting textbooks or physically distributing update packages. This ensures that learners always have access to the most current information while significantly reducing the long-term maintenance costs of training.

**30.** (D) Enabling the transfer of courses and content between different learning systems
Content packaging is a fundamental aspect of e-learning standards that ensures portability and interoperability. It establishes a standardized structure for bundling instructional materials, metadata, and sequencing rules into a single file. This allows educational content to be seamlessly transferred and correctly interpreted by different learning management systems, protecting an organization's investment in digital instructional assets across various technological platforms.

**31.** (C) Web Safari automatically restricts learners from seeing the instructor's pointer during browsing
In a virtual classroom, the Web Safari tool is specifically designed to enhance visibility by showing the instructor's pointer to all students. This synchronization ensures that learners can follow the instructor's actions, including scrolling and highlighting, in real-time. Therefore, claiming that the feature restricts students from seeing the pointer is inaccurate, as it serves the exact opposite instructional purpose.

**32.** (B) Manual inventory management
Virtual classrooms are designed to facilitate interactive and collaborative online learning through features like voice conferencing, breakout rooms for group work, and Web Safari for synchronized browsing. Manual inventory management, which involves tracking physical items like textbooks or lab equipment, is a logistical task typical of traditional brick-and-mortar institutions and is not a standard feature within a digital classroom platform.

Downloaded from www.pdf.tube

**49.** (A) Floppy Disk Distribution
Modern e-learning trends post-Covid focus on digital and internet-based methodologies such as mobile learning, gamification, and video-based instruction. Floppy disk distribution is an obsolete technology from several decades ago and is not part of current or emerging educational strategies. Today's learning environments rely on high-speed internet and cloud-based storage to deliver interactive and engaging content to a global audience.

**50.** (C) Vulnerability
The development of the SCORM standard was driven by several key objectives including accessibility, durability, interoperability, and reusability. These goals ensure that learning content is portable and long-lasting across different systems. Vulnerability, which refers to weaknesses in security or system stability, is not an objective of the standard; rather, developers work to minimize vulnerabilities to ensure a secure learning environment.

**51.** (D) Small instructional units reusable across different learning contexts
Learning objects are built on the concept of modularity and reusability. These small, self-contained digital units are designed to address specific learning objectives. Because they are standardized, they can be easily combined with other objects to create diverse courses. This approach allows organizations to save time and resources by reusing high-quality instructional components across various training programs and different platforms.

**52.** (D) The Psychomotor domain is concerned with growth in feelings or emotional areas
In Bloom's Taxonomy, the psychomotor domain is actually focused on manual or physical skills, such as coordination and movement. Growth in feelings, attitudes, and emotional areas is addressed by the affective domain instead. Understanding these distinctions is essential for instructional designers to ensure they are targeting the correct type of learning behavior through their specific educational objectives and assessment strategies.

**53.** (C) The ability to completely eliminate the need for physical office buildings
While e-learning offers numerous benefits such as cost savings, 24/7 accessibility, and instant content updates, it does not inherently eliminate the need for physical office buildings. Organizations still require infrastructure for administrative staff, equipment maintenance, and various business operations. E-learning reduces the reliance on physical classrooms for training, but it is not a complete solution for removing institutional spaces.

NODIA

**54.** (C) An arrangement of resources and procedures to promote learning
An instructional system is comprehensively defined as a coordinated arrangement of human resources, technological tools, and procedural methods designed to facilitate and promote learning. It involves a systematic approach to analyzing needs and developing strategies to achieve specific educational goals. This holistic view ensures that all components work together effectively to create a successful and measurable learning environment for students in various settings.

**55.** (A) Intuitive
Bloom's Taxonomy classifies educational objectives into three primary domains: cognitive, affective, and psychomotor. "Intuitive" is not one of the established categories in this framework. The cognitive domain covers mental skills, the affective domain deals with emotional growth, and the psychomotor domain involves physical actions. These three domains provide a comprehensive structure for defining and measuring various types of learning behaviors.

**56.** (A) It exclusively develops standards that are only applicable to and used by the aviation industry
Although AICC originated within the aviation industry, its standards were widely adopted across many different sectors globally. The committee's work, particularly in computer-managed instruction, provided foundational guidelines that influenced the broader e-learning field. Therefore, stating that its standards are exclusively applicable only to aviation is incorrect, as they achieved significant cross-industry relevance before the organization's functions were eventually transferred.

41. (A) Analyze, Design, Develop, Implement, Evaluate
The ADDIE model follows a systematic five-stage sequence for instructional design. It begins with Analysis to define needs, followed by Design to plan objectives and strategies. Development involves creating the actual materials, which are then used during the Implementation phase. Finally, the Evaluation phase assesses the effectiveness of the training. This order ensures that each step informs the next for success.

42. (C) Experience API statements can only be stored within a Learning Management System (LMS)
Experience API statements are not restricted to storage within a traditional Learning Management System. Instead, they are typically stored in a specialized system called a Learning Record Store. An LRS can operate independently or as a component within an LMS. This flexibility allows the tracking of learning experiences across diverse environments, including mobile applications, physical hardware, and various third-party platforms.

43. (B) Increasing the physical travel requirements for hands-on labs
One of the primary objectives of a virtual classroom is to reduce or eliminate the need for physical travel. By providing a digital space for collaboration and instruction, these platforms make education more accessible and cost-effective. Increasing travel requirements would be contradictory to the goals of improving efficiency and accessibility, which are central to the implementation of virtual learning environments.

44. (D) Graphic Interface Design
E-learning standards are generally categorized into technical areas that ensure system compatibility and data exchange. These include metadata for content labeling, content packaging for course transfer, and learner profiles for sharing personal data. While graphic interface design is crucial for user experience, it is considered a design preference or aesthetic choice rather than a standardized technical interoperability category for cross-system communication.

45. (C) Using learning analytics to provide data for the Learning and Development path
Interactive content as an emerging trend offers the significant advantage of generating detailed learning analytics. These data points allow organizations to track how users engage with specific elements of a course. By analyzing these interactions, Learning and Development managers can make informed decisions to optimize instructional paths, tailor content to learner needs, and improve the overall effectiveness of training programs.

46. (B) LCMS manages the process of scheduling classes, creating catalogues, and registering learners
The tasks of scheduling classes, maintaining course catalogs, and managing learner registrations are administrative functions typically performed by a Learning Management System. A Learning Content Management System instead focuses on the creation, management, and storage of the learning content itself. While both systems are related, their primary operational focuses are distinct within the architecture of a standard e-learning infrastructure.

47. (B) The experiences and contexts that make the student willing and able to learn
In the field of instructional design, readiness refers to a learner's state of preparation for a specific educational experience. This includes having the necessary prior knowledge, life experiences, and environmental contexts that enable them to engage with and successfully acquire new information. Understanding a learner's readiness helps designers create materials that are appropriate for their current level of ability and motivation.

48. (B) Anonymous feedback is not possible in a Virtual Classroom, unlike a traditional classroom
Anonymous feedback is actually a key feature of virtual classrooms, often being easier to implement than in traditional physical settings. Digital tools allow students to respond to polls or provide comments without their identity being revealed to peers. This encourages honest input and participation from learners who might otherwise feel hesitant to speak up or disagree in a public, face-to-face environment.

Click Here to Buy book on Amazon

update, and deliver educational components to different platforms and diverse target audiences.

**17.** (A) A protocol using statements formatted as 'actor, verb, and object'
The Experience API, often referred to as Tin Can API, utilizes a specific data format to track learning activities. It records interactions as simple statements consisting of an actor, a verb, and an object. This structure allows the system to capture a wide range of learning experiences occurring both inside and outside traditional learning environments with high flexibility and precision.

**18.** (A) 480 kbps
High-performance virtual classroom environments often utilize adaptive video bandwidth to ensure a smooth user experience for all participants. To achieve the highest possible performance for this feature, a minimum connection speed of 480 kbps is generally required. This bandwidth ensures that video streams remain stable and clear even when multiple interactive tools and collaborative features are used simultaneously.

**19.** (D) Motivating learners by presenting their training as an engaging 'play thing'
Organizations integrate gamification into their learning platforms to increase engagement and motivation among employees. By applying game-design elements like points, badges, and leaderboards, training is presented as an engaging and interactive experience. This approach transforms traditional instructional content into a more enjoyable format, encouraging learners to participate more actively and complete their assigned educational pathways with higher interest.

**20.** (A) Affordability
Affordability is a primary objective of the SCORM standard, focusing on the economic benefits of digital learning. It aims to increase organizational efficiency and productivity by minimizing the time and expenses required to deliver and manage instructional content. By standardizing the way content is handled, organizations can reduce development costs and optimize their overall training budget across different delivery platforms.

**21.** (C) A tool provided free of charge to anyone wishing to test content conformance
The SCORM Conformance Test Suite is a vital resource provided by the Advanced Distributed Learning initiative. This diagnostic software is made available free of charge to developers and organizations globally. Its primary purpose is to verify whether learning content and management systems correctly implement the technical specifications required for SCORM compliance, ensuring seamless interoperability and consistency across different platforms.

**22.** (B) Aviation Industry CBT Committee
The acronym AICC represents the Aviation Industry Computer-Based Training Committee. This international organization was originally formed to develop guidelines for the aviation industry's training materials. Over time, its work became influential across various sectors, leading to the creation of standards that ensure interoperability between different computer-based training systems and management platforms used in corporate and academic settings worldwide.

**23.** (D) Allowing learners to complete training faster, thereby increasing individual productivity
E-learning provides a distinct advantage for fast learners compared to traditional, synchronous classroom settings. By offering self-paced modules, it allows individuals to progress through materials at their own speed. Those who grasp concepts quickly can finish their training earlier than scheduled, which enhances their individual productivity and allows them to return to their primary job responsibilities much sooner than usual.

**24.** (D) A standardized method for integrating rich learning applications with platforms
Learning Tools Interoperability is a standard developed by the IMS Global Learning Consortium. It provides a consistent and secure method for connecting external learning applications and tools with educational platforms like Learning Management Systems. By using LTI, organizations can seamlessly integrate various third-party resources, such as simulations or assessments, into a unified and cohesive learning environment for their students.

NODIA

**57.** (A) Ensuring content reusability across courses and LMSs without constraints
The primary benefit of SCORM standardization is the guarantee of content reusability and interoperability. It allows instructional materials to be created once and then successfully deployed across various learning management systems without the need for expensive redesign or reprogramming. This flexibility protects an organization's investment by ensuring their digital assets are not locked into a single proprietary software vendor or platform.

**58.** (A) It is a proprietary, closed-source learning management system
Moodle is actually an open-source Learning Management System, not a proprietary or closed-source one. It is distributed under the GNU General Public License, allowing users to freely download, modify, and share the software. This open nature has led to a large global community of developers and educators who contribute to its continuous improvement and the creation of numerous functional plugins.

**59.** (C) To provide standardized data structures and protocols for cross-system work
E-learning standards aim to establish common data structures and communication protocols that enable different educational technologies to work together seamlessly. By following these rules, developers ensure that content created in one tool can be tracked and managed by various management systems. This interoperability reduces costs, prevents vendor lock-in, and facilitates the efficient sharing of instructional resources across disparate organizational platforms.

**60.** (B) HTML
AICC, IEEE, and ADL are all recognized organizations or initiatives that develop and maintain technical standards for the e-learning industry. HTML, which stands for HyperText Markup Language, is a coding language used to create web pages. While it is a standard for web content, it is not an organization that accredits or develops specific e-learning interoperability frameworks like SCORM.

**61.** (C) P-3, Q-4, R-1, S-2
Mobile learning leverages smartphone ubiquity for personalized learning. Video-based learning grew exponentially after the pandemic breakout. Gamification presents training as an engaging 'play thing' to motivate learners. Interactive content uses analytics to shape instructional paths. This matching reflects the current landscape of digital education, where technology enhances engagement and provides data-driven insights for better overall learning outcomes and organizational efficiency.

**62.** (A) Only (I) is correct
Statement (I) is correct because digital tools in virtual classrooms facilitate anonymous feedback, allowing students to share honest opinions without hesitation. Statement (II) is incorrect because raising hands in a traditional classroom is a public act that reveals a student's identity and choice to everyone present. Thus, the virtual environment offers a unique advantage for gathering genuine, unbiased participant views.

**63.** (A) P-3, Q-1, R-4, S-2
Accessibility involves locating and delivering components remotely. Adaptability is the ability to tailor instruction to specific needs. Durability refers to adding content without costly technological redesigns. Reusability involves extracting and reassembling modules into new courses. These objectives define the technical requirements for content to be effectively managed and shared across various learning management systems while protecting long-term educational investments.

**64.** (C) ((I) and (III) only)
Statement (I) is correct as mobile learning remains underexplored despite widespread smartphone use globally. Statement (III) is correct because interactive strategies use learning analytics to inform content development. Statement (II) is false because gamification is designed to motivate and allure learners, not deter them. Therefore, trends focusing on personalization and data-driven insights are the accurate characteristics highlighted in this context.

**65.** (A) Design - Choose an instructional approach
In the ADDIE model, the design phase involves creating a blueprint for the training, which

Downloaded from www.pdf.tube

and tasks, followed by the design of objectives and strategies, the trainer ensures a structured approach to curriculum development. This model is widely recognized for its effectiveness in creating comprehensive and targeted training programs in both corporate and academic settings.

**100.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
SCORM requires that courses run on different systems because the goal of interoperability is to ensure that instructional components are functional across various platforms. The ability to use tools and content from different locations is the core definition of interoperability within the standard. Therefore, the explanation in the reason accurately supports why the requirement in the assertion exists for digital learning.

**101.** (A) Video-based Learning
Video-based learning is the specific method that gained immense prominence and grew at an exponential rate following the Covid-19 breakout. This approach became indispensable as organizations and educational institutions shifted toward digital delivery to maintain continuity. The visual and engaging nature of video content made it a preferred medium for delivering information effectively to learners who were working remotely during lockdowns.

**102.** (A) (I), (II), (III), and (V) only
Statements (I), (II), (III), and (V) correctly describe the pandemic's impact on e-learning, its indispensable nature, the personalization of mobile learning, and the motivational role of gamification. Statement (IV) is incorrect because video-based learning actually gained prominence after the pandemic rather than losing it. These trends reflect the rapid digital transformation that occurred in the learning and development sector globally.

**103.** (B) Learning Objects
The technical term for small, reusable digital instructional components is learning objects. These units are designed to be self-contained and modular, allowing them to be utilized in multiple courses or contexts. By using learning objects, designers can efficiently create varied instructional programs while ensuring that high-quality content is consistently applied across the organization's different learning and content management systems.

**104.** (C) Assertion (A) is true, but Reason (R) is false.
While it is true that virtual classrooms enable anonymous feedback through digital tools, the claim that traditional physical classrooms allow the same process seamlessly is false. In a face-to-face setting, gestures like raising hands or speaking up are inherently public. Achieving true anonymity in a physical classroom typically requires more complex manual methods, unlike the integrated features found in digital learning.

**105.** (C) Shared whiteboards
Shared whiteboards are the specific virtual classroom feature that allows instructors to annotate pre-prepared materials live. These interactive markups can be saved, providing a valuable resource for students to review later. This functionality enhances the learning experience by combining structured content with dynamic, real-time explanations, while also saving time for the instructor during the actual synchronous session with students.

NODIA

**106.** (A) (I), (II), and (III) only
Statements (I), (II), and (III) accurately describe HTML as a de facto standard, the role of IEEE in de jure standards, and how SCORM integrates various specifications. Statement (IV) is incorrect as LTI typically involves a tool provider and a tool consumer. Statement (V) is also false because the SCORM Test Suite is provided free of charge by the ADL.

**107.** (A) Psychomotor
The psychomotor domain in Bloom's Taxonomy is the specific category that encompasses manual and physical skills. These objectives focus on coordination, motor skills, and the physical actions required to perform tasks, such as operating a new machine. By identifying these skills within the psychomotor domain, trainers can design more effective hands-on exercises and assessments to ensure learners gain the necessary proficiency.

74. (C) Cognitive - Knowledge
In the alignment between Bloom's Taxonomy and the KSA model, the cognitive domain corresponds directly to knowledge. The affective domain relates to attitude, and the psychomotor domain corresponds to skills. This mapping helps instructional designers categorize learning objectives accurately to ensure that training addresses the intended type of development, whether it is mental, emotional, or physical in nature for learners.

75. (B) (I), (III), and (IV) only
Statements (I), (III), and (IV) correctly identify AICC's role in CBT guidelines, IMS's focus on metadata, and ADL's U.S. government sponsorship. Statement (II) is incorrect because SCORM was developed by ADL, not exclusively by IEEE LTSC, although it incorporates IEEE standards. These organizations work together to create a unified framework for interoperability and content management in the digital learning industry.

76. (D) P-2, Q-4, R-3, S-1
AICC is an international group originally focused on aviation CBT. IEEE LTSC provides specifications like the LOM. IMS focuses on metadata tagging and content packaging. ADL is the government-sponsored organization that developed SCORM. Each entity plays a specialized role in establishing the technical rules that allow different learning technologies and content to interoperate effectively across diverse organizational and educational platforms.

77. (B) ((I) and (III) only)
Statement (I) is correct as the taxonomy was proposed in 1956. Statement (III) is also correct because learning behaviors represent the goals of training. Statement (II) is incorrect because the affective domain deals with emotions and attitudes, while manual or physical skills belong to the psychomotor domain. Understanding these domain boundaries is critical for setting appropriate educational goals and assessments for students.

78. (D) P-3, Q-4, R-2, S-1
An LMS manages administrative tasks like user registration. An LCMS handles the creation and reuse of digital content. LTI integrates external applications with platforms. An LRS stores experiential data statements. These different components and standards work together within a modern learning ecosystem to provide a comprehensive experience for both administrators and learners while ensuring data is recorded and shared accurately.

79. (B) Only (II) is correct
Statement (II) is correct as video-based learning saw a massive rise in prominence following the Covid-19 breakout. Statement (I) is incorrect because the e-learning industry did not come to a halt; instead, it experienced unprecedented growth as it became the primary means for education globally. The pandemic acted as a catalyst that accelerated the adoption of digital technologies across all sectors.

80. (D) Durability - Reducing the time and costs involved in delivering instructional content
The description provided for durability actually refers to the objective of affordability. Durability is focused on ensuring that learning content remains functional and does not require redesign when underlying technologies change. Affordability is specifically about the economic efficiency and cost-effectiveness of delivering training. Correctly identifying these objectives is essential for implementing the SCORM standard effectively in organizations to protect educational investments.

81. (A) ((I), (II), and (III) only)
Statements (I), (II), and (III) correctly identify the core activities of analysis, design, and development within the ADDIE framework. Statement (IV) is false because evaluation is an ongoing part of the cyclical process, not a one-time event that ends the cycle permanently. The results of evaluation are used to inform future iterations and improvements to the instructional materials and overall strategy.

82. (A) P-3, Q-4, R-1, S-2
Voice conferencing provides integrated multi-way audio. Shared whiteboards allow for interactive and savable markups. Web Safari enables synchronized web browsing. Breakout rooms are used for dividing sessions into team exercises. These features collectively create a rich, collaborative environment that supports

Click Here to Buy book on Amazon

# CHAPTER 09
# Banking Software

May/June 2023

**1.** Match the characteristics of an international commercial Banking System in List I with their descriptions in List II:
List I: Characteristics
P. Multi-Currency
Q. Multi-Entity
R. Multi-Branch
S. Bulk Transaction Entry
List II: Descriptions
1. Permits amounts to be entered in foreign currency and allows currency revaluation.
2. Supports institutions to profile regional, country, and subsidiary operations.
3. Provides for 24 × 7 real-time transaction processing of clearings and payments.
4. Supports inter-location and inter-bank activity including different time zones.

(A) P-2, Q-1, R-3, S-4
(B) P-4, Q-3, R-1, S-2
(C) P-1, Q-4, R-2, S-3
(D) P-1, Q-2, R-4, S-3

Oct/Nov 2014

**2.** In a core banking solution, the 'store and forward' facility is designed to ensure that:
(A) Transactions are delayed intentionally to verify anti-money laundering compliance.
(B) All data is stored permanently on the branch server while the central server acts as a backup.
(C) Branches can continue to function locally without hindrance during a breakdown of connectivity.
(D) Customer requests are routed strictly through an offline clearinghouse before processing.

May/June 2019

**3.** Which of the following best represents the function of Non-Banking Financial Institution software within the banking software categorization?
(A) Handling payroll, pension, and provident fund
(B) Reconciling inter-branch transactions
(C) Managing mutual funds, portfolios, and capital
(D) Monitoring asset liability management and non-performing assets

NODIA

Oct/Nov 2006

**4.** A Web server is best defined as a program that:
(A) Backend database specifically used for managing relational records
(B) Physical routing of network packets across various Wide Area Networks
(C) Uses HTTP to serve files that form Web pages to users
(D) Consolidating funds from multiple locations into a single bank account

May/June 2021

**5.** Identify the incorrect statement concerning exception processing in the application of fees/ charges.
(A) It provides greater flexibility by allowing fees to be applied across the board effecting all accounts.
(B) Implementation of fee variations strictly at the regional management level
(C) Variations of fees implemented exclusively by specific product or account type
(D) Variations of fees implemented at the account type or transaction event level

Oct/Nov 2010

**6.** The primary function of an Application Server in a typical data center arrangement is to act as the middleman between:
(A) The network router and the external internet service provider
(B) Browser-based front-ends and back-end database legacy systems
(C) The magnetic storage devices and the optical storage devices
(D) The domain controller and the desktop clients

**91.** (B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
While both statements are true, the 24/7 availability of materials is not the direct cause of fast learners finishing early. Fast learners finish sooner because the self-paced nature of e-learning allows them to move quickly through the content once they understand it. Round-the-clock access is a separate logistical benefit that provides flexibility for when learning can occur for all students.

**92.** (C) SCORM (Shareable Content Object Reference Model)
SCORM is specifically designed to ensure that digital learning content is reusable and portable across different management systems. By following this model, organizations like aviation institutes can protect their intellectual capital from being locked into a single proprietary platform. It allows instructional components to be moved seamlessly between different delivery systems while maintaining full functionality and accurate tracking of all student progress.

**93.** (B) (I), (II), (III), and (IV) only
Statements (I) through (IV) correctly describe the finalization of xAPI 1.0, its data format, the role of the LRS, and cmi5 as a companion released in 2016. Statement (V) is incorrect because cmi5 was developed to improve interoperability within traditional LMS environments using xAPI, not to eliminate the LMS entirely. It provides the necessary structure for modern tracking in legacy systems.

**94.** (C) Web Safari
The professor is using the Web Safari feature, which is specifically designed for synchronous online web tours. This tool allows the instructor to lead learners through a website, where their actions like scrolling and pointing are mirrored on the students' screens. It ensures that everyone in the virtual session remains synchronized and focused on the same online resources during the instructional period.

**95.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Virtual classrooms reduce travel and facility costs because they enable large groups to collaborate and learn within a digital environment. By removing the need for physical presence in a specific location, organizations avoid the significant expenses associated with transportation, venue rentals, and physical infrastructure. Thus, the collaborative nature of the digital environment directly explains why it is a cost-effective solution.

**96.** (B) Gamification
The manager is adopting gamification, an emerging trend that uses game-design elements to increase motivation and engagement. By presenting training as an interactive and engaging "play thing," learners are more likely to participate and complete their modules. This approach transforms the perception of mandatory training into a more enjoyable experience, ultimately leading to better retention and a higher return on investment.

NODIA

**97.** (A) ((I), (III), and (IV) only)
Statements (I), (III), and (IV) correctly identify e-learning's delivery methods, its cost-saving potential, and the ability to use extensive colorful graphics. Statement (II) is false because LMS platforms are specifically designed to track student answers automatically. Statement (V) is incorrect as e-learning typically removes time zone restrictions by providing 24/7 access to materials, allowing for a more flexible schedule.

**98.** (A) Learning Record Store (LRS)
A Learning Record Store is the specialized data repository required to save and query experiential statements generated using the "actor verb object" format. While an LMS handles administrative tasks, the LRS focuses specifically on storing and managing the granular tracking data produced by various learning activities. This system allows for more comprehensive tracking of experiences that occur across diverse digital platforms.

**99.** (B) The ADDIE Model
The trainer is following the ADDIE model, which is a systematic five-phase process for instructional design. By starting with the analysis of learners

**116.** (A) (I), (II), (III), and (V) only
Statements (I), (II), (III), and (V) correctly identify that virtual classrooms promote active learning, support ad-hoc discussions, function on low bandwidth, and offer audience control tools. Statement (IV) is incorrect because virtual classrooms typically encourage the sharing of applications to enhance interactive learning rather than preventing it for security reasons. These capabilities combine to create a versatile and engaging online environment.

**117.** (D) Breakout rooms
Breakout rooms are the virtual classroom feature used to split a main session into smaller groups for team collaboration or individual exercises. This allows students to work together without distracting others, while the instructor retains the ability to monitor and join these sub-sessions as needed. This tool effectively replicates the small-group dynamics found in physical classrooms, facilitating deeper interaction and collaborative peer learning.

**118.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Instructional design is a systematic process because it ensures quality by analyzing needs and developing a delivery system to meet them. By translating general learning principles into specific materials, designers create a more effective educational experience. The detailed analysis and development described in the reason are exactly what make the process systematic, as stated in the initial assertion about design.

**119.** (A) Learning Record Store (LRS)
To save and query experiential data statements formatted in the "actor verb object" style, a dedicated data store called a Learning Record Store is essential. Unlike a traditional management system, the LRS is built specifically to handle the high-volume, granular tracking data produced by the xAPI standard. It provides a central hub for analyzing learning that occurs across diverse digital environments.

**120.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Mobile learning is considered underexplored because there is a vast, untapped potential within the four billion smartphone users globally. The ubiquity of these devices provides an ideal platform for delivering personalized, on-demand training. This massive user base is the direct reason why the trend is viewed as underestimated, as the reach and frequency of mobile access are globally unparalleled.

**121.** (D) Moodle
The client is using Moodle, which is a prominent free and open-source Learning Management System. It is written in PHP and distributed under the GNU General Public License. Designed on pedagogical principles, Moodle allows institutions to create a highly customized and flexible learning environment. Its open-source nature means that it is supported by a global community and can be easily expanded.

**122.** (C) Durability
The developer is aiming to meet the objective of durability. This SCORM goal ensures that instructional materials remain functional as technology evolves, allowing new content to be added or infrastructure to be upgraded without requiring costly redesigns or recoding. By adhering to this standard, the developer guarantees that the module is a long-term investment that survives changes in the client's technology environment.

**123.** (C) cmi5
The companion specification to xAPI released in 2016 is called cmi5. It was developed to provide a standardized set of rules for how xAPI should be used within traditional Learning Management Systems. By implementing cmi5, organizations can achieve interoperability for their digital content while benefiting from the advanced tracking capabilities and flexible data format offered by the underlying xAPI protocol.

**124.** (A) Interoperability
The ability to run a module on any platform and combine components from different locations is the core of the interoperability objective. SCORM ensures that content is not restricted to

Downloaded from www.pdf.tube

**108.** (C) Assertion (A) is true, but Reason (R) is false.
HTML is a de facto standard because it has achieved widespread use through industry adoption rather than through an initial stamp of approval from an accrediting body like IEEE. While organizations like the W3C now maintain its specifications, its status as a standard originally came from being used by a critical mass of developers globally, rather than from a formal de jure certification.

**109.** (D) Experience API (Tin Can API / xAPI)
The Experience API, also known as Tin Can API or xAPI, is the appropriate standard for tracking learning data in a flexible "actor verb object" format. It is specifically designed to record experiences outside traditional web browsers, such as those occurring in simulators or mobile apps. This flexibility allows for a more comprehensive understanding of a learner's activities across diverse digital environments.

**110.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
SCORM acts as a force multiplier for designers because the standardization increases efficiency while reducing time and costs. By providing a consistent framework, it allows developers to focus on the quality of content rather than technical compatibility issues. This efficiency and the resulting improvements in student comprehension directly explain why standardization is so beneficial for the overall instructional design process.

**111.** (D) Interactive Content
The use of learning analytics to inform and shape the instructional path is a hallmark of the interactive content trend. By analyzing how learners interact with digital materials, organizations can gain valuable insights into their progress and difficulties. This data allows for the creation of more personalized and effective learning experiences, helping managers optimize their overall training strategy and achieve better educational outcomes.

**112.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
E-learning provides significant cost savings primarily because digital materials can be updated and distributed without the recurring expenses of physical production. By avoiding the costs of reprinting books, maintaining physical inventory, and manual distribution, organizations can maintain current training at a much lower price point. This efficiency is a direct reason why e-learning is financially advantageous for many modern institutions.

**113.** (C) Assertion (A) is true, but Reason (R) is false.
While Bloom's Taxonomy does divide objectives into cognitive, affective, and psychomotor domains, the reason provided is incorrect. The affective domain is concerned with emotional growth, feelings, and attitudes, rather than manual or physical skills. Manual or physical skills are the focus of the psychomotor domain. Understanding these clear distinctions is necessary for the accurate application of the taxonomy in education.

**114.** (B) Develop
The phase in the ADDIE model where instructional or training materials are physically created is called Development. During this stage, the plans and strategies from the design phase are turned into actual learning products, such as modules, presentations, or handouts. This is a critical step where the instructional vision becomes a reality before it is implemented with the intended student audience.

**115.** (D) Learning Content Management System (LCMS)
A Learning Content Management System is the specific tool designed to allow designers to author, sequence, and aggregate digital content. It facilitates collaboration by enabling multiple subject matter experts to share and reuse small instructional components across various courses. This focus on content-level management distinguishes it from a traditional LMS, which is more concerned with the administrative aspects of learner registration.

NODIA

various instructional methods and allows for real-time interaction between all participants, enhancing the overall effectiveness of virtual classroom sessions.

**83.** (D) P-4, Q-1, R-3, S-2
CAM stands for Content Aggregation Model. RTE stands for Run-Time Environment. KSA represents Knowledge, Skills, and Attitude. xAPI is also known as the Tin Can API. These terms and acronyms are fundamental to the technical and pedagogical frameworks used to design, deliver, and track modern digital learning experiences across different platforms while ensuring consistent data communication and interoperability.

**84.** (D) (I), (II), and (III)
All three statements are correct. Metadata supports indexing and discovery. Content packaging defines rules for delivery to learners. Learner profiles facilitate the communication of user data like scores and completion status. Together, these categories form the technical foundation for interoperability, allowing different systems to understand and process learning content and data in a consistent and reliable manner for organizational success.

**85.** (A) Both (I) and (II) are correct
Statement (I) correctly notes that Experience API statements are saved in a Learning Record Store (LRS). Statement (II) is also accurate as an LRS can function as a standalone system or be integrated within an LMS. This architectural flexibility is a key feature of the xAPI standard, allowing for tracking of learning activities across a wide variety of digital contexts.

**86.** (B) P-3, Q-4, R-1, S-2
The cognitive domain is associated with knowledge. The affective domain involves growth in emotional areas. The psychomotor domain focuses on skills. Finally, attitude is the KSA equivalent of the affective domain. This alignment ensures that educational designers can categorize and target different aspects of human development using consistent terminology and frameworks to achieve specific and measurable training goals for learners.

**87.** (A) (I), (II), and (IV) only
Statements (I), (II), and (IV) correctly identify the administrative role of an LMS, the delivery focus of an LCMS, and how LCMS data is passed back to the LMS. Statement (III) is incorrect because authoring and sequencing tools are features of an LCMS, not a standard LMS. These systems are designed to complement each other in a full-scale digital learning ecosystem.

**88.** (B) P-3, Q-1, R-4, S-2
Audience control lets teachers manage microphones. Feedback tools enable anonymous responses for honest views. Live tests provide tracked assessments and reports. Live presentation tools incorporate various media like Flash and GIFs. These digital capabilities offer unique pedagogical benefits that are often difficult or impossible to replicate effectively in a traditional physical classroom setting, enhancing engagement and providing valuable performance data.

**89.** (C) (I) and (III) only
E-learning provides flexibility and convenience in the learning process. Fast learners can complete courses more quickly because training is often self-paced, making Statement I correct. It also allows learners to access study materials anytime and anywhere, ensuring 24/7 accessibility, so Statement III is correct. However, Statement II is incorrect because e-learning generally expands training opportunities and reduces resource constraints rather than limiting staff training. Therefore, only Statements I and III are correct.

**90.** (A) IMS - Primarily focuses on developing web browser software
IMS Global Learning Consortium does not focus on developing web browser software. Instead, it is an organization dedicated to creating technical standards and specifications for learning technologies, such as metadata and content packaging. The other options correctly link AICC with CMI guidelines, IEEE with LOM, and ADL with the SCORM model. Understanding these roles is vital for navigating modern e-learning implementation.

Click Here to Buy book on Amazon

a single management system, allowing it to be used across diverse technological environments. This standard allows organizations to source or develop instructional materials independently of the specific delivery platform they choose to use.

**125.** (B) LTI (Learning Tools Interoperability)
Learning Tools Interoperability is the standard specifically designed to integrate rich learning applications with educational platforms. It allows a system to act as a consumer that can securely launch and receive data from external third-party tools. By using LTI, multinational corporations can seamlessly incorporate specialized simulations, assessments, or other interactive resources into their unified learning management environment for all employees.

NODIA

includes choosing the appropriate instructional approach and defining learning objectives. Other phases have different focuses: Analyze assesses needs and learner characteristics, Develop involves creating the actual materials, and Implement is the actual delivery. Evaluation determines if the goals were met. Thus, design correctly maps to strategy.

**66.** (A) ((I), (II), and (III) only)
Statements (I), (II), and (III) accurately describe accessibility for locating content, adaptability for tailoring instruction, and affordability for reducing delivery costs. Statement (IV) is incorrect because durability specifically aims to ensure that content does not need a complete redesign when technology evolves. By adhering to these objectives, organizations can create sustainable and efficient digital learning environments that survive technological changes.

**67.** (B) ((II), (I), (III))
The Experience API was initially released before it was finalized to version 1.0 in April 2013. The cmi5 specification, which serves as a critical companion to xAPI, was released later in 2016. This sequence reflects the progressive development of tracking standards in the e-learning industry, moving from initial concepts to finalized specifications and subsequent specialized companion rules for platform interoperability.

**68.** (A) Only (I) is correct
Statement (I) correctly identifies that a Learning Content Management System focuses on managing digital content for delivery to the right people. Statement (II) is incorrect because authoring and aggregation tools are primary features of an LCMS, not a standard LMS. An LMS is typically responsible for administrative tracking, while the LCMS handles the detailed structure and reuse of educational content.

**69.** (B) ((II) and (III) only)
Statements (II) and (III) are correct because Moodle is an open-source PHP platform under the GNU license that supports community plugins for customization. Statement (I) is false as Moodle is the opposite of a proprietary, closed-source system. Its popularity stems from this openness, allowing institutions to tailor the environment to their specific pedagogical needs while benefiting from global contributions.

**70.** (C) P-2, Q-4, R-1, S-3
Metadata focuses on labeling for indexing and discovery. Content packaging enables course transfer between systems. Learner profiles allow for sharing personal data and scores. Accrediting organizations include groups like AICC, IEEE, and ADL. These categories organize complex technical requirements into manageable areas that ensure digital learning materials are functional and portable across different platforms, protecting an organization's instructional investment.

**71.** (D) ((I), (II), (III), and (IV))
All provided statements accurately describe virtual classroom features. Voice conferencing is integrated and full duplex. Whiteboards allow for saving interactive markups. Web Safari enables synchronized browsing led by the instructor. Breakout rooms provide smaller collaborative spaces where the instructor can maintain control and oversight. Together, these tools replicate and enhance the interactive dynamics of a physical classroom in a digital environment.

**72.** (B) P-4, Q-3, R-2, S-1
Analysis involves assessing learner characteristics and tasks. Design focuses on developing objectives and instructional approaches. Development is the phase where instructional materials are created. Evaluation ensures that the materials achieved their intended goals. This systematic progression ensures that training is built on a solid foundation and achieves measurable success for the target audience by addressing specific educational needs and requirements.

**73.** (D) Both (I) and (II) are incorrect
Statement (I) is incorrect because instructional design is typically the starting point, not the final stage. Statement (II) is incorrect as the ADDIE model is a cyclical, iterative process rather than one where phases end permanently. The evaluation phase often leads back to analysis for continuous improvement. Thus, instructional design is an ongoing, systematic effort to refine and enhance materials.

Downloaded from www.pdf.tube

May/June 2005

**7.** Which of the following is categorized under Reconciliation and settlement software?
(A) Comprehensive Credit Risk Management systems
(B) RTGS
(C) Centralized pension fund management modules
(D) Automated refinance management protocols

Oct/Nov 2022

**8.** Consider the following statements regarding Interest and Base Rate Processing in a banking system:
I The system allows for table selected and banded rates which may be set from a prime rate.
II Interest capitalisation is restricted solely to the end of the term.
III Base rates and base rate margins can apply individually by product type and category.
IV Base rates can apply globally across all product types and categories.
Which of the above statements are correct?
(A) (I), (II), and (III)
(B) (I), (III), and (IV)
(C) (II), (III), and (IV)
(D) (I), (II), (III), and (IV)

May/June 2018

**9.** The Centralized Money Management (CMM) service provides several benefits. Which of the following is NOT one of those benefits?
(A) Consolidating funds for the purpose of maximizing investment opportunities
(B) Daily reports that increase administration and telephone costs
(C) Providing banking flexibility by allowing cash deposits at any local branch
(D) Simplifying reconciliation by uniquely identifying each specific branch location

Oct/Nov 2016

**10.** The following question consists of two statements: Assertion (A) and Reason (R). Choose the correct option based on these statements.
Assertion (A): The Performance Management utility in a banking system is used to monitor system capacity and manage growth.
Reason (R): As new products are introduced and volumes grow, benchmarks must be performed to ensure continued satisfactory response to end-users.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2014

**11.** Which of the following is an example of an open-source Application Server from the JBoss community?
(A) Oracle Weblogic
(B) Sun Glassfish
(C) IBM Websphere
(D) JBoss

Oct/Nov 2007

**12.** Identify the correct statement regarding the core of an Integrated Banking System (IBS).
(A) A flat file system specifically designed to contain isolated customer records
(B) Hard-coded operational instructions that operate without using master tables
(C) Relational database systems using standard codes stored in master tables
(D) Security management module bypasses to ensure faster transaction processing

May/June 2025

**13.** Centralized banking solutions, also known as core banking solutions, are generally based on:
(A) Open system, multi-tier architecture for seamless integration
(B) Closed proprietary network infrastructures with single-tier architecture
(C) Decentralized mainframe processing without any branch server connectivity
(D) Batch-processing mechanisms that exclusively perform updates at end-of-day

NODIA

Oct/Nov 2019

**14.** Which facility allows a customer to quote an account number and password over the telephone to automatically generate cheques debited to a savings account?
(A) Direct Debit Facility
(B) Sweeps Processing

any external wide area network systems

**May/June 2009**

**57.** Which of the following technologies is NOT prominently recognized as a primary driver of 'value chain disruption' in the FinTech sector?
(A) Quantum Computing
(B) Artificial Intelligence (AI)
(C) Blockchain
(D) Robotic Process Automation (RPA)

**Oct/Nov 2011**

**58.** Cloud storage presents several advantages and disadvantages. Which of the following is NOT a 'Con' (disadvantage) of Cloud storage?
(A) Vulnerability to local physical disasters such as theft and floods
(B) High operational costs compared to purchasing traditional external hard drives
(C) Requirement of an ongoing subscription model to maintain data accessibility
(D) Significantly slower data transfer rates compared to other local backup systems

**May/June 2010**

**59.** Consider the following statements about downloading files from file hosting websites:
I Paid premium plans typically remove speed and bandwidth limitations imposed on free users.
II A premium plan guarantees download speeds that exceed the maximum capacity provided by the user's local ISP.
Which of the above statement(s) is/are correct?
(A) Only (I) is correct
(B) Only (II) is correct
(C) Both (I) and (II) are correct
(D) Neither (I) nor (II) is correct

**Oct/Nov 2024**

**60.** According to the guidelines for a successful online banking web site, internal navigation is a characteristic that ensures:
(A) Restricting users to sequential page viewing only for security reasons
(B) Navigating between pages with links back to the main homepage
(C) Automatic debiting of account maintenance fees during active user sessions
(D) Blocking all website pages that attempt to open in new browser windows

**May/June 2017**

**61.** Concerning regulatory guidelines on digital lending, identify the correct statement regarding customer grievances.
(A) The guidelines leave grievance redressal strictly to the customer's local police station.
(B) Grievance redressal is optional for loan disbursements below a certain threshold.
(C) Appointment of a Nodal Grievance Officer to address customer grievances is made mandatory.
(D) Complaints must be routed through international cybercrime agencies.

**Oct/Nov 2005**

**62.** The following question consists of two statements: Assertion (A) and Reason (R). Choose the correct option based on these statements.
Assertion (A): In an Integrated Banking System, password encryption and branch location checks are integral to user access validation.
Reason (R): Data security ensures that signing on with a user number and password automatically guarantees unconditional access to all applications and functions.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2020**

**63.** Determine the correct chronological sequence of steps involved in a BaaS process.
I The startup uses the API to build new Fintech apps.
II A financial institution providing BaaS opens its API to the startup.
III A Fintech startup pays a fee to access a BaaS platform.
(A) (II), (III), (I)
(B) (III), (II), (I)
(C) (I), (II), (III)
(D) (III), (I), (II)

Click Here to Buy book on Amazon

modules of different functions such as loans and deposits.

II The IBS architecture excludes communication interface systems to maintain data privacy.

Which of the above statement(s) is/are correct?

(A) Only (I) is correct
(B) Only (II) is correct
(C) Both (I) and (II) are correct
(D) Neither (I) nor (II) is correct

**May/June 2013**

**23.** Consider the following statements regarding the generic charging system in the Fees and Charges module:

I It supports a tiered flat charge based on transaction values.

II It allows for geographic tables to enforce uniform charge rates across all areas.

III It provides the capability to exempt individual account holders from specific fees.

Which of the above statement(s) is/are correct?

(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

**Oct/Nov 2021**

**24.** A bank in India analyzed customer data to discover that a significant proportion of business was coming from upwardly mobile women, leading to the launch of a targeted credit card. This scenario illustrates which advantage of centralized banking software?

(A) Execution of local 'store and forward' system mechanisms
(B) Simplified administration of the global 'Push' sweep facility
(C) Implementation of the centralized Base Rate Processing module
(D) Use of predictive analytics on customer behaviour data

**May/June 2024**

**25.** A high-net-worth individual instructs their bank to automatically transfer any balance exceeding ₹50,000 in their savings account to a designated investment account. Which sweep facility is the customer utilizing?

(A) Pull sweep
(B) Push sweep
(C) On line sweep
(D) Offset sweep

**Oct/Nov 2008**

**26.** An Integrated Banking System architecture is designed primarily to ensure that the system is:

(A) Tightly coupled with the underlying platform to prevent external tampering
(B) Dependent on standalone processing nodes without any central synchronization
(C) Exclusively tailored to support a single local currency and a single entity
(D) Robust, expandable, and platform-isolated

**May/June 2006**

**27.** Match the Web Servers in List I with their corresponding characteristics in List II:

List I: Web Servers

P. Apache Web Server
Q. IIS Web Server
R. Nginx Web Server
S. Web Container

List II: Characteristics

1. Microsoft product where personal modules cannot be added easily.
2. Uses a highly scalable event-driven architecture instead of threads.
3. Open source software containing a modular structure that runs on a large percentage of machines.
4. Part of the application server architecture receiving servlet requests.

(A) P-3, Q-1, R-2, S-4
(B) P-1, Q-3, R-4, S-2
(C) P-2, Q-4, R-1, S-3
(D) P-3, Q-2, R-1, S-4

**Oct/Nov 2017**

**28.** Zenith Bank operates across three continents. Recently, the bank decided to consolidate its General Ledger systems into one central computer at a regional processing centre while allowing individual subsidiaries to run their own base currencies and local reporting. Which capability of their commercial Banking System allows for this specific operational structure?

(A) Multi-Entity support
(B) Multi-Lingual control
(C) High Availability Operation
(D) Bulk Transaction Entry

Downloaded from www.pdf.tube

(C) Phone Pay/Bill Pay
(D) Mobile IVR Setup

May/June 2009

**15.** Identify the correct statement regarding the Nginx Web Server.
(A) It is primarily an operating system used for banking mainframes.
(B) It uses a multithreaded architecture that consumes vast amounts of memory under load.
(C) It restricts modifications and is strictly maintained by Microsoft.
(D) It is a free open source web server known for high performance and low resource usage.

Oct/Nov 2011

**16.** In a bank's software ecosystem, deploying multiple independent application software instead of an integrated banking software typically results in:
(A) Time-consuming integration and inadequate level of support
(B) Reduced integration time and superior bank support
(C) Seamless data synchronization across all independent modules
(D) Elimination of the need for specialized IT personnel

May/June 2010

**17.** Consider the following statements regarding the benefits of Core banking for banks:
I Process standardization within bank & branches.
II Accuracy in transactions & minimization of errors.
III Improved management of documentation resulting in quick gathering of MIS reports.
IV Increased operational costs due to continuous server upgrades.
V Ease in submission of various reports to the Government & Regulatory bodies.
Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (V)
(B) (I), (II), (III), and (IV)
(C) (II), (III), (IV), and (V)
(D) (I), (III), (IV), and (V)

Oct/Nov 2024

**18.** A commercial Banking System utilized for international operations must possess several key characteristics. Which of the following is NOT typically one of these required characteristics?
(A) Compulsory manual recovery from all hardware failures to ensure data integrity
(B) Platform independence
(C) Capability to facilitate the use of APIs in delivery channel management
(D) In-built fault tolerant features to leverage clustered multi-processing architectures

May/June 2017

**19.** Identify the correct pair regarding the benefits of centralized banking.
(A) Benefit for Customers - Reduced need for hardware independence
(B) Benefit for Banks - Increased transaction turnaround times for safety
(C) Benefit for Banks - Exclusivity of branch-level standalone databases
(D) Benefit for Customers - Anywhere banking by eliminating branch banking

NODIA

Oct/Nov 2005

**20.** In the context of banking software security, user access validation is best characterized by which of the following?
(A) Sign-on/off at terminal levels with user capability recognized post sign-on
(B) Full access to all applications immediately following the initial sign-on process
(C) Universal passwords utilized across all branch locations for simultaneous access
(D) Static password structures that remain unchangeable once established by the bank

May/June 2020

**21.** Identify the incorrect pair regarding server types and their functions.
(A) Web Server - Forwards HTTP responses to the Web Client
(B) Application Server - Hosts business layer logic and complex transaction-based applications
(C) Database Server - Middleman formatting HTML pages directly for user interfaces
(D) Application Server - Works with approaches like Common Gateway Interface (CGI)

Oct/Nov 2015

**22.** Consider the following statements regarding the Integrated Banking System (IBS):
I The base tables are populated by program

through an Ethernet port.
III It utilizes multiple SAN switches known as SAN directors.
IV It can be set up with RAID to increase reliability.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (III)
(B) (I), (II), and (IV)
(C) (II), (III), and (IV)
(D) (I), (III), and (IV)

**Oct/Nov 2023**

**36.** Digital-only or neo-banks exist solely in the virtual world. The primary operational characteristic of a neo-bank in India is that:
(A) It operates as a banking correspondent and technology service provider to traditional banks.
(B) It functions as a fully licensed central bank managing physical currency distribution.
(C) It can directly accept large corporate deposits and offer massive lending products on its own books.
(D) It is totally exempt from central bank regulations or oversight.

**May/June 2016**

**37.** An Application Administrator (AA) is primarily responsible for:
(A) Building and maintaining the server and resolving helpdesk issues
(B) Modifying database structures while managing complex data replication tasks
(C) Designing relational tables and issuing SQL queries for backend data storage
(D) Developing the underlying operating systems used for local branch computers

**Oct/Nov 2009**

**38.** Connection speed, or Internet Bandwidth, refers strictly to:
(A) The exact rate at which files are written to a user's local hard drive.
(B) The speed of the server hosting the requested file.
(C) The time taken for an application server to fetch data from a database.
(D) The raw data transfer rate of the connection provided by the ISP.

**May/June 2023**

**39.** Torrent downloads differ from conventional downloads. Which of the following is NOT a characteristic of torrent-based downloading?
(A) It relies on a peer-to-peer (P2P) model.
(B) Data flows universally among connected users known as peers.
(C) Having more seeders than leechers can potentially increase download speed.
(D) Download speed depends strictly on a single central client-server node.

**Oct/Nov 2025**

**40.** Consider the following statements regarding SAN storage:
I SANs are typically switched fabric architectures using Fiber Channel (FC) for connectivity.
II SAN storage provides synchronous replication which is a key requirement for disaster recovery strategy.
Which of the above statement(s) is/are correct?
(A) Only (I) is correct
(B) Only (II) is correct
(C) Both (I) and (II) are correct
(D) Neither (I) nor (II) is correct

**May/June 2012**

**41.** A customer wants to open a wealth account that allows him to invest in zero commission mutual funds while offering a high interest rate on savings. He chooses a 2-in-1 digital savings account. Which neo-bank product does this describe?
(A) Fi
(B) Niyo
(C) Justwealth
(D) Saxo

**Oct/Nov 2018**

**42.** The following question consists of two statements: Assertion (A) and Reason (R). Choose the correct option based on these statements.
Assertion (A): A Windows domain allows users to use enhanced security for their VPN connections.
Reason (R): When a domain is added to a network, it supports a certification authority enabling the use of smart cards and digital certificates.
(A) Both Assertion (A) and Reason (R) are true,

Click Here to Buy book on Amazon

May/June 2008

**29.** The following question consists of two statements: Assertion (A) and Reason (R). Choose the correct option based on these statements.
Assertion (A): Centralized Return generation reduces the time and cost compared to a distributed banking solution.
Reason (R): In a distributed banking solution, consolidating financial statements from multiple locations for submission to the central bank is a lengthy and costly process.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Oct/Nov 2013

**30.** A corporate client of Apex Bank has a global facility backed by multiple collateral assets. The client requests a new loan utilizing a portion of the collateral. The bank's system ensures the collateral is only pledged up to its nominated value by linking it against other entities. Which management system handles this functionality?
(A) Base Rate Processing System
(B) Exception Processing System
(C) Performance Management System
(D) Collateral Management System

May/June 2015

**31.** Match the category of storage device in List I with its specific example in List II:
List I: Storage Device
P. Magnetic storage
Q. Optical storage
R. Flash memory
S. Cloud storage
List II: Example
1. Blu-ray disc
2. Floppy diskette
3. Amazon S3
4. Solid State Drive (SSD)
(A) P-1, Q-2, R-3, S-4
(B) P-4, Q-3, R-2, S-1
(C) P-2, Q-1, R-4, S-3
(D) P-2, Q-1, R-3, S-4

NODIA

Oct/Nov 2012

**32.** Match the factor affecting download speed in List I with its description in List II:
List I: Factor
P. Packet delivery method
Q. Server load
R. Routing
S. Network Interface Controller (NIC)
List II: Description
1. Shortest path selection affecting bandwidth based on distance.
2. Hardware adapter limitations on the client device side.
3. Throttling of connection due to too many parallel requests on the host.
4. Overhead consumed by message headers attached to downloaded data.
(A) P-3, Q-4, R-2, S-1
(B) P-4, Q-3, R-1, S-2
(C) P-1, Q-2, R-3, S-4
(D) P-4, Q-1, R-3, S-2

May/June 2011

**33.** An IT professional in a bank is tasked with testing the network for weaknesses, implementing email filters, and installing security programs. Based on these duties, what role is the professional performing?
(A) Database Administrator
(B) Network Administrator
(C) Application Administrator
(D) Content Manager

Oct/Nov 2020

**34.** In calculating download speed from connection speed, which mathematical progression is accurately applied?
(A) Divide Megabits by 8 to get Kilobytes directly.
(B) Multiply Megabytes by 1024 to get Megabits, then multiply by 8 to get Kilobytes.
(C) Divide Megabits by 1024, then multiply by 8.
(D) Multiply Megabits by 1024 to get Kilobits, then divide by 8 to get Kilobytes.

May/June 2022

**35.** Consider the following characteristics regarding Network Attached Storage (NAS):
I It uses IDE or SATA hard drives plugged in an array storage enclosure.
II It connects to a network Router or Hub

(C) A server serving too many parallel requests might throttle connections.
(D) Message headers in data packets take up a portion of the downloaded data, effectively reducing the net file download rate.

**Oct/Nov 2022**

**50.** The following question consists of two statements: Assertion (A) and Reason (R). Choose the correct option based on these statements.
Assertion (A): A bank's Internet presence is much more accessible than its brick and mortar location.
Reason (R): A bank web site can easily be visited by anyone worldwide who has access to a computer.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2018**

**51.** The following question consists of two statements: Assertion (A) and Reason (R). Choose the correct option based on these statements.
Assertion (A): Neo-banks cannot accept deposits or offer lending products on their own books.
Reason (R): Neo-banks do not hold full-fledged banking licenses and must partner with non-banking financial companies or traditional banks.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2016**

**52.** If a bank needs to integrate PCs running a non-Windows operating system into a Windows domain, which open source package is identified as a suitable alternative to facilitate this?
(A) Active Directory
(B) Glassfish
(C) FastCGI
(D) Samba

**May/June 2014**

**53.** Global Bank requires a highly resilient, highly scalable storage solution that supports synchronous replication to ensure robust business continuity for critical block-level data across clustered virtual servers. Which storage architecture is most appropriate?
(A) Tape cassette storage
(B) Single External Hard Drives
(C) Storage Area Network (SAN)
(D) Simple Network Attached Storage (NAS)

**Oct/Nov 2007**

**54.** Identify the correct statement regarding torrent terminology.
(A) Seeder - A user who is only downloading data from the network
(B) Leecher - A user who is uploading data into the network
(C) Seeder - A user who is uploading data into the network
(D) Node - A central server that strictly controls all data flow without peers

**May/June 2025**

**55.** When measuring connection speed and download speed, different units are employed. The relationship between these metrics is rooted in the fact that:
(A) Relationship where 8 bits equal 1 byte, making Kilobytes smaller
(B) Relationship where 1 bit equals 8 bytes, making download speeds larger
(C) Megabits are for local network storage while Megabytes are for routing
(D) Connection speed equals disk read/write speed regardless of units used

**Oct/Nov 2019**

**56.** In the context of networking, a domain is defined as:
(A) Group of computers administered as a unit with common rules
(B) Localized hard drive dedicated specifically to automated backup operations
(C) Maximum download bandwidth available through an external internet connection
(D) Standalone computer disconnected from

Downloaded from www.pdf.tube

and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2007**

**43.** A bank customer subscribes to a 2 Mbps internet connection. Assuming no external or internal limiting factors, what is the theoretical maximum download speed they should expect in KBps?
(A) 128 KBps
(B) 256 KBps
(C) 512 KBps
(D) 2000 KBps

**Oct/Nov 2014**

**44.** In the context of designing an online banking web site, the component referred to as "look" is primarily concerned with:
(A) Internal navigation links and the efficiency of online form submission
(B) Search engine algorithms and background logic for HTTP server processing
(C) Physical accessibility and geographical location of a brick and mortar branch
(D) Graphical design, attractiveness, and first impressions of personality

**May/June 2019**

**45.** Based on user surveys, which of the following mobile banking features are considered most valuable?
(A) Real-time stock trading and integrated cryptocurrency exchange services
(B) Automatically sending international physical cheques via postal services
(C) Fingerprint login and the ability to place temporary holds on cards
(D) Generating high-volume bulk transaction entries for clearinghouse systems

**Oct/Nov 2006**

**46.** Consider the following tasks related to data management:
I Monitoring and optimizing the performance of the database.
II Planning for backup and recovery of database information.
III Providing technical support to wireless remote data terminals.
Which of the above tasks fall under the responsibilities of a Database Administrator (DBA)?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

**May/June 2021**

**47.** The following question consists of two statements: Assertion (A) and Reason (R). Choose the correct option based on these statements.
Assertion (A): Download managers can often improve the overall downloading speed of a file.
Reason (R): Download managers set up multiple connections in parallel to download several parts of the file simultaneously, provided the server allows it.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2010**

**48.** Identify the correct statement distinguishing Network Attached Storage (NAS) from Storage Area Networks (SANs).
(A) NAS provides block-level access, whereas SAN provides file-level access services
(B) NAS provides file-level access, whereas SAN provides block-level access
(C) SAN connects through standard IDE hard drives without using fabric switches
(D) NAS is strictly an offline backup method that cannot be connected to any LAN

**May/June 2005**

**49.** Identify the incorrect statement regarding factors that affect internet download speeds.
(A) A faster connection speed guarantees maximum download speed even if the local Disk Read/Write Speed is extremely slow.
(B) Operating system background services can consume bandwidth, reducing download speed.

NODIA

Oct/Nov 2015

**64.** Identify the correct statements regarding core banking implementation mandates by regulatory bodies:

I A deadline was mandated for Urban Co-operative Banks (UCBs).

II The deadline for UCBs to implement CBS was December 31, 2013.

III Regional Rural Banks (RRBs) were completely exempt from implementing CBS.

IV The requirement was driven by the need to cope with growing customer needs.

V The deadline was met by all RRBs and UCBs.

Which of the above statement(s) is/are correct?

(A) (I), (II), (IV), and (V)
(B) (I), (II), (III), and (IV)
(C) (II), (III), (IV), and (V)
(D) (I), (III), (IV), and (V)

May/June 2013

**65.** Consider the following statements regarding vendor selection criteria:

I Accessibility relates to how easily the vendor's services can be obtained, often because the company is local.

II Pricing Options reflect the vendor's openness to fixed-price versus variable-price contracts.

Which of the above statement(s) is/are correct?

(A) Only (I) is correct
(B) Only (II) is correct
(C) Both (I) and (II) are correct
(D) Neither (I) nor (II) is correct

Oct/Nov 2021

**66.** A financial organization needs to host middle-tier business logic and scheduled jobs for their complex transaction-based applications. They must select a server capable of providing distributed application services. Which server type is most suitable?

(A) Application Server
(B) Static Data Store
(C) Simple NAS Storage
(D) Web Container

May/June 2024

**67.** A gig economy worker needs a customized, small ticket loan quickly without visiting a branch. Which category of financial institution is currently best placed to use advanced technologies to provide this specific service?

(A) Traditional Brick-and-Mortar Banks
(B) Central Banks
(C) Neo Banks
(D) Inter-Branch Clearinghouses

Oct/Nov 2008

**68.** Consider the following components integrated into a commercial Banking System:

I Retail components

II E-Commerce components

III Treasury and Trade components

IV MIS components

Which of these enable effective international deployment?

(A) (I), (II), and (III)
(B) (II), (III), and (IV)
(C) (I), (III), and (IV)
(D) (I), (II), (III), and (IV)

May/June 2006

**69.** Centralized banking solutions offer multiple delivery channels. Consider the following examples:

I ATM

II Mobile banking

III Tele-banking

Which of the above are standard delivery channels in a centralized banking solution?

(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

Oct/Nov 2017

**70.** Match the vendor selection criteria in List I with their specific definitions in List II:

List I: Criteria

P. Industry Knowledge
Q. Banking IT Knowledge
R. Application Familiarity
S. Project Management

List II: Definition

1. Understanding features of a specific vendor's application package being installed.
2. Managing scheduling, budgeting, and deliverables responsibilities.
3. Understanding regulations, industry consolidation, and competition in banking.
4. Understanding data center consolidations, distributed architectures, and GroupWare.

Click Here to Buy book on Amazon

(A) P-4, Q-3, R-2, S-1
(B) P-3, Q-1, R-4, S-2
(C) P-3, Q-4, R-1, S-2
(D) P-2, Q-4, R-1, S-3

May/June 2008

**71.** The following question consists of two statements: Assertion (A) and Reason (R). Choose the correct option based on these statements.
Assertion (A): A database administrator (DBA) is expected to stay abreast of emerging technologies and new design approaches.
Reason (R): A DBA's responsibilities involve capacity planning, installation, security, and modifying the database structure based on application developer inputs.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Oct/Nov 2013

**72.** Robo Advisory in investment banking is best described as:
(A) Use of android robots at teller counters to manage cash deposit transactions
(B) Robotic investment technology providing broad services with minimum investment
(C) Exclusive use of human advisors augmented by standard banking calculators
(D) High-cost alternatives aimed only at ultra-high-net-worth corporate accounts

May/June 2015

**73.** Identify the incorrect pair regarding application functions in the Integrated Banking System.
(A) Phone Pay - Generates cheques automatically based on telephone inputs
(B) Inquiries - Handles title details and insurance details
(C) Fees and Charges - Supports tiered flat charges based on transaction values
(D) Sweeps - Manages collateral assignment against global facilities

Oct/Nov 2012

**74.** In the context of Integrated Banking System architecture, which of the following is NOT an external interface shown connected to the Communications Interface System?
(A) SWIFT
(B) ATM
(C) Mainframe Tape Drive
(D) Call Center

May/June 2011

**75.** Identify the incorrect statement regarding Web Servers.
(A) Apache is an open source software installed on operating systems like Linux, UNIX, and Windows.
(B) IIS server has features like Apache, but personal modules cannot be added easily.
(C) Considerations in choosing a Web server include security characteristics and ability to handle server-side programming.
(D) Nginx uses threads to handle requests, resulting in highly unpredictable memory usage.

Oct/Nov 2020

**76.** Consider the following statements regarding the Bank-as-a-Service (BaaS) model:
I BaaS enables FinTech startups to connect to a bank's system through APIs.
II It requires FinTechs to purchase and build their own heavy infrastructure before launching.
III An established bank allows Fintechs to launch new services on top of its existing regulated infrastructure.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

NODIA

May/June 2022

**77.** Identify the correct statement regarding the elements of Core Banking Solutions (CBS) that help customers.
(A) Fund transfers through NEFT and RTGS are excluded from CBS elements.
(B) CBS forces customers to visit their own branch for routine transactions.
(C) Mobile banking operates independently and cannot integrate with CBS.

(D) POS and kiosk systems are considered basic elements of CBS.

**Oct/Nov 2023**

**78.** The following question consists of two statements: Assertion (A) and Reason (R). Choose the correct option based on these statements.
Assertion (A): Timely regulation measures on Fintech are designed to avoid restricting innovation while preventing harm to enterprises.
Reason (R): Acting too early would have restricted innovation, while waiting too long would have allowed harmful practices to evolve beyond an easy return.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2016**

**79.** The Base Rate Processing system supports the addition, deletion, and maintenance of base rates. How can these base rate margins be applied?
(A) Only individually by product type
(B) Either individually by product type and category or globally
(C) Only globally across all product categories
(D) Strictly at the end of the financial year

**Oct/Nov 2009**

**80.** A bank customer executes a foreign exchange transaction that requires calculation in both the Base Currency and a foreign currency. The system immediately calculates and extracts the figures without requiring manual batch processing. This illustrates the system's capability in:
(A) Multi-Lingual support
(B) Bulk Transaction Entry
(C) Sweeps execution
(D) Multi-Currency operations

**Oct/Nov 2025**

**81.** Application servers provide multiple approaches to forward a request from a web server. Which of the following is NOT one of those approaches?
(A) Common Gateway Interface (CGI)
(B) Java Server Page
(C) Internet Control Message Protocol (ICMP)
(D) Microsoft's Active Server Page

**May/June 2012**

**82.** Consider the following points regarding standard guidelines on Digital Lending:
I Prohibiting data scraping from consumer phones.
II Obtaining explicit consent for data collected for lending.
III Upfront disclosure of all costs involved.
IV Mandatory automated credit limit increases.
V A cooling-off period for borrowers to exit digital loans.
Which of the above are standard components of digital lending regulations?
(A) (I), (II), and (III), and (IV)
(B) (I), (II), and (III), and (V)
(C) (II), (III), (IV), and (V)
(D) (I), (III), (IV), and (V)

**May/June 2005**

**83.** A bank is selecting an IT vendor to migrate its legacy system to a distributed architecture. The selection committee emphasizes the vendor's prior history of successfully working with the bank on a "preferred vendor" basis. Which specific criterion is the bank prioritizing?
(A) Accessibility
(B) Pricing Options
(C) Technical Skills
(D) Incumbency

**Oct/Nov 2010**

**84.** Consolidated Returns and reports in a centralized solution drastically reduce time and cost because:
(A) Branch-level standalone statements must be physically mailed to the office
(B) The system completely eliminates the need for any formal regulatory reporting
(C) Immediate consolidation of statements at the central server
(D) It employs non-structured data scraping from individual consumer phone devices

**May/June 2021**

**85.** The Inquiries module in the banking application supports various basic types of inquiries. Which

NODIA

of the following is NOT typically listed as a supported inquiry type?
(A) Short Inquiries
(B) Advances History Inquiries
(C) Non-Customer External Debit Inquiries
(D) Security Document Movement Inquiries

**Oct/Nov 2006**

**86.** Artificial Intelligence in Fintech benefits various backend and middle office operations. Which of the following is NOT typically listed as one of these AI-benefited processes?
(A) Risk assessment
(B) Physical branch layout design
(C) Anti-fraud measures
(D) Credit underwriting

**May/June 2019**

**87.** Match the web server components in List I with their interactions in List II:
List I: Component
P. Web Client
Q. Application Server
R. Web Container
S. Static Data Store
List II: Interaction
1. Returns Servlet Response to the Web Server.
2. Provides Static Data Response to the Web Server.
3. Sends HTTP Request to the Web Server.
4. Houses the Web Container and Application Data Store interactions.
(A) P-4, Q-3, R-2, S-1
(B) P-3, Q-4, R-1, S-2
(C) P-3, Q-1, R-4, S-2
(D) P-1, Q-2, R-3, S-4

**Oct/Nov 2014**

**88.** Identify the incorrect statement regarding vendor selection criteria for IT services in banking.
(A) Security Standards evaluation of the vendor's internal organizational structure
(B) Irrelevance of incumbency because banks always prefer new vendors for IT
(C) Track Record measurements via reference customers and industry-wide reputation
(D) Total Cost comparisons with competitors for the delivery of equivalent services

**May/June 2007**

**89.** A bank manager notices that branch servers are continuing to function normally and store intermediate transactions during an unexpected WAN outage. The central database will sync up once the network is restored. This scenario is a practical application of:
(A) Pull Sweep Processing
(B) Store and forward facility
(C) FastCGI integration
(D) Multi-Entity processing

**Oct/Nov 2018**

**90.** The core of an Integrated Banking System (IBS) relies heavily on standard codes. Where are these standard codes typically stored?
(A) In different master tables (e.g., Position, gaps, ALM codes)
(B) In the temporary RAM of the branch server
(C) In isolated text files on each employee's desktop
(D) In the external cloud storage provided by ISPs

**May/June 2023**

**91.** A website designer for City Bank creates a clear site map, incorporates an internal search engine, and ensures every page has links back to the main page. These actions specifically improve which characteristic of the website?
(A) Graphic attractiveness
(B) Internal navigation
(C) Bandwidth limitation
(D) Base Rate Processing

**Oct/Nov 2016**

**92.** During an IT vendor selection process for managing a data center consolidation, the bank assesses how well the vendor understands the shift from legacy systems to distributed architectures. Which specific criterion is the bank evaluating?
(A) Incumbency
(B) Track Record
(C) Banking IT Knowledge
(D) Pricing Options

**May/June 2014**

**93.** In the evolution of storage devices, why did Flash memory start to replace magnetic media?
(A) Flash memory relies exclusively on paper storage methods which are cheaper
(B) Flash memory utilizes lasers and lights for

Downloaded from www.pdf.tube

writing data unlike magnetic storage
(C) Flash memory became cheaper, faster, and more reliable than magnetic media
(D) Flash memory requires no electricity to function within electronic systems

**Oct/Nov 2007**

**94.** When implementing a 'store and forward' facility for branch connectivity in a core banking environment, what is a primary performance requirement during local processing mode?
(A) Shutdown for 10 minutes
(B) Users will be logged out automatically
(C) There should be no impact upon on-line response times to end users
(D) All transaction fees will double during processing

**May/June 2025**

**95.** Identify the correct statement regarding FinTech app usage as per recent global studies.
(A) Filing a card transaction dispute is considered low priority by modern users
(B) Most mobile users research bank app capabilities before opening accounts
(C) Physical banks are successfully avoiding the need to launch any Fintech apps
(D) Biometric logins like fingerprints are being phased out in modern Neo-banks

**Oct/Nov 2019**

**96.** Match the type of software in List I with its respective module in List II:
List I: Software Type
P. Core banking software
Q. MIS related software
R. Reconciliation and settlement software
S. Non-Banking Financial Institution software
List II: Module
1. Electronic Clearance System (ECS)
2. Refinance management
3. Deposits and advances treasury
4. ALM, NPA, Credit Risk Management
(A) P-4, Q-3, R-2, S-1
(B) P-3, Q-4, R-1, S-2
(C) P-3, Q-1, R-4, S-2
(D) P-1, Q-2, R-3, S-4

**May/June 2009**

**97.** Consider the following tasks related to system management:
I Generating reports and database queries using VB script.
II Designing the physical brick and mortar layout of new branches.
III Maintaining metadata and supporting document management facility.
IV Providing technical support to web designers.
Which of the above are standard responsibilities of an Application Administrator?
(A) (I), (II), and (IV)
(B) (I), (III), and (IV)
(C) (II), (III), and (IV)
(D) (I), (II), (III), and (IV)

**Oct/Nov 2011**

**98.** Identify the expected impacts of Artificial Intelligence (AI) in financial institutions from the following statements:
I Dealing with the growing menace of cybercrime and financial frauds.
II Leveraging chatbots for customer support services.
III Benefiting middle office processes like anti-fraud.
IV Cost-effectiveness resulting in optimized internal processes.
V Eradicating the need for any human employees by 2025.
Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (IV)
(B) (I), (II), (IV), and (V)
(C) (II), (III), (IV), and (V)
(D) (I), (III), (IV), and (V)

NODIA

**May/June 2010**

**99.** Identify the incorrect statement concerning "Technical Skills" in the IT vendor selection criteria.
(A) It involves assessing the vendor's ability to use specific software tools.
(B) It measures the geographical proximity of the vendor's local service office.
(C) It evaluates proficiency in specific techniques and programs.
(D) It determines the level of expertise the vendor has with required products.

**Oct/Nov 2024**

**100.** A Bit is the fundamental unit of data representation. Why is connection speed usually measured in Megabit per second (Mbps) rather than Megabyte per second (MBps)?

typically results in time-consuming integration efforts and an inadequate level of technical support from various vendors. Without a unified system, data synchronization becomes difficult, increasing the risk of errors and making it harder to maintain a consistent database.

**17.** (A) (I), (II), (III), and (V)
Core banking implementation offers several key benefits for financial institutions, including the standardization of processes across all branches. It enhances transaction accuracy and minimizes errors while improving documentation management for faster gathering of MIS reports. Additionally, centralized data simplifies the submission of required reports to regulatory bodies and the government, though it should be noted that operational costs might increase.

**18.** (A) Compulsory manual recovery from all hardware failures to ensure data integrity
An international commercial banking system must be robust, platform-independent, and capable of utilizing APIs for delivery channel management. It should leverage fault-tolerant features and clustered architectures to ensure high availability. Expecting compulsory manual recovery from hardware failures is contrary to the goals of modern systems, which prioritize automated recovery processes to maintain data integrity and minimize downtime in critical operations.

**19.** (D) Benefit for Customers - Anywhere banking by eliminating branch banking
Centralized banking provides significant advantages for both financial institutions and their clients. For customers, one of the most prominent benefits is the ability to perform 'anywhere banking,' which eliminates the traditional constraints of being tied to a specific branch location. By accessing a central database, users can manage their accounts and conduct transactions seamlessly from any branch or digital interface.

**20.** (A) Sign-on/off at terminal levels with user capability recognized post sign-on
Security in banking software involves rigorous user access validation procedures. This typically includes requiring a sign-on and sign-off at terminal levels, where the system recognizes specific user capabilities only after a successful authentication. This granular approach ensures that employees can only access the applications and functions authorized for their role, protecting sensitive financial data from unauthorized use or accidental modifications.

**21.** (C) Database Server - Middleman formatting HTML pages directly for user interfaces
While web servers handle HTTP requests and application servers host business logic, database servers are primarily responsible for storing and retrieving data records. It is incorrect to describe a database server as a middleman that formats HTML pages directly for user interfaces. That formatting role belongs to the web or application layer, whereas the database server focuses on executing complex queries efficiently.

**22.** (A) Only (I) is correct
The architecture of an Integrated Banking System relies on program modules from various functions, such as loans and deposits, to populate central base tables. This ensure data consistency across the entire organization. However, the claim that IBS architecture excludes communication interface systems is false, as these interfaces are essential for connecting the core system to external networks like SWIFT and ATMs.

**23.** (C) (I) and (III) only
A generic charging system in a banking environment offers flexibility by supporting tiered flat charges based on the specific value of transactions. It also provides the capability to grant exemptions to individual account holders for specific fees based on their profile or relationship with the bank. However, enforcing uniform charge rates across all geographic areas would limit the system's necessary local adaptability.

**24.** (D) Use of predictive analytics on customer behaviour data
Predictive analytics is a powerful tool within centralized banking software that allows institutions to analyze customer behavior and identify trends. By examining data from their entire customer base, banks can discover specific market segments, such as upwardly mobile women, and design targeted financial products like specialized credit cards. This data-

Click Here to Buy book on Amazon

(D) Simple Web Client

May/June 2024

**107.** High Availability Operation in a banking system ensures that recovery from hardware failures is almost completely automatic. This implies that:
(A) Complex manual recovery procedures are no longer necessary.
(B) Programmers must constantly write new code to incorporate fault tolerance.
(C) The system deliberately slows down online response times during peak hours.
(D) Fault tolerant hardware platforms are rendered obsolete.

Oct/Nov 2008

**108.** In understanding download speeds from internet connections, several external server-side factors can reduce the practical rate. Which of the following is NOT an external server-side factor?
(A) Network Interface Controller (NIC) limitations on the user's device
(B) Server capacity
(C) Packet delivery method and message headers
(D) Routing and distance from the server

May/June 2006

**109.** Why are Neo banks addressing their regulatory predicament by outsourcing their banking responsibilities and creating strategic partnerships with traditional banks?
(A) Requirement that traditional banks supply them with core banking software
(B) Handling corporate foreign exchange transactions exclusively for global firms
(C) Total shutdown of all physical branch locations by traditional banking firms
(D) Lack of licenses preventing them from accepting deposits on their own

Oct/Nov 2017

**110.** A FinTech company wishes to launch a new payment app. Instead of purchasing heavy infrastructure and obtaining a banking license, it pays a fee to an established bank to access its regulated platform through APIs. This operational strategy is known as:
(A) Cloud Storage Virtualization
(B) Distributed Torrent Network
(C) Bank-as-a-Service (BaaS)
(D) Centralized Sweep Processing

May/June 2008

**111.** Identify the correct statement regarding "Multi-Branch" support in a commercial banking system.
(A) Branch IDs are typically merged into the customer ID structure.
(B) Inter-bank activity is strictly disallowed to prevent SWIFT address conflicts.
(C) All branches must operate in the exact same time zone and base currency.
(D) Each processing entity has an ID structure that is unique and separate from any part of the account or customer ID structure.

Oct/Nov 2013

**112.** Consider the following statements regarding online banking web site features:
I The "feel" of a site refers to the ability to move back and forth easily and efficiently fill out non-obtrusive forms.
II Customers expect the web site to offer a safe, attractive environment comparable to a brick and mortar bank.
Which of the above statement(s) is/are correct?
(A) Only (I) is correct
(B) Only (II) is correct
(C) Both (I) and (II) are correct
(D) Neither (I) nor (II) is correct

May/June 2015

**113.** Consider the following statements regarding the mechanics of torrent downloads:
I It replaces the client-server model with a peer-to-peer (P2P) model.
II Leechers are users who are strictly uploading data into the network.
III Numerous active parallel connections are utilized to download parts of the data simultaneously.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (I) and (III) only
(C) (II) and (III) only
(D) (I), (II), and (III)

Oct/Nov 2012

**114.** Consider the following parameters used in setting up "Exception processing" for fees and charges:
I Account type

NODIA

II Interest category
III Transaction event level
IV Customer's physical height
Which of the above statement(s) is/are correct?
(A) (I), (II), and (III)
(B) (II), (III), and (IV)
(C) (I), (III), and (IV)
(D) (I), (II), and (IV)

**May/June 2011**

**115.** Determine the correct chronological sequence to calculate download speed in Kilobytes per second (KBps) from a connection speed given in Megabits per second (Mbps):
I Divide by 8 to convert from Kilobit (Kb) to Kilobyte (KB).
II Identify the connection speed in Megabits (Mb).
III Multiply the connection speed by 1024 to convert from Megabit (Mb) to Kilobit (Kb).
(A) (II), (I), (III)
(B) (II), (III), (I)
(C) (III), (II), (I)
(D) (I), (II), (III)

**Oct/Nov 2020**

**116.** Match the storage network terms in List I with their features in List II:
List I: Terms
P. Network Attached Storage (NAS)
Q. Storage Area Networks (SANs)
R. Cloud Storage
S. RAID
List II: Features
1. Commercial data center space accessed via the internet, serving as a good offsite backup.
2. File-level access architecture plugged into a Router or Hub.
3. Block-level access connected behind servers using switched fabric architectures.
4. Setup providing redundancy that increases reliability and read/write performance.
(A) P-3, Q-2, R-4, S-1
(B) P-1, Q-4, R-3, S-2
(C) P-2, Q-1, R-4, S-3
(D) P-2, Q-3, R-1, S-4

**May/June 2022**

**117.** Consider the following functions in a bank:
I Payroll
II Personal information system
III Pension
IV Provident fund
V Inter Branch Reconciliation (IBR)
Which of the above functions are typically managed under a bank's administration software?
(A) (I), (II), (III), and (IV)
(B) (II), (III), (IV), and (V)
(C) (I), (III), and (IV)
(D) (I), (II), (IV), and (V)

**Oct/Nov 2023**

**118.** A user is attempting to download a large file from a file hosting site. Despite having a high-speed internet plan, the download speed is strictly capped at a low rate. The user is using a free regular account on the hosting site. What is the primary cause of this limitation?
(A) The user's internal random access memory is overflowing during the session
(B) The torrent swarm has too many seeders actively uploading the requested file
(C) The Network Interface Controller has failed completely on the client device
(D) Speed caps imposed by the server on regular, non-premium user accounts

**May/June 2016**

**119.** Match the innovative product/feature in List I with its corresponding Neo/Digital bank application in List II:
List I: Product/Feature
P. High interest rate and zero forex markup
Q. Spare change investment tool
R. Voice-enabled finance tracking
S. Small ticket credit products
List II: Application
1. Aimed at gig economy workers and tech-savvy millennials.
2. Allows users to convert their spare change into investments.
3. Provided as part of a 2-in-1 Digital Savings account.
4. Voice-enabled search and finance tracking tool.
(A) P-3, Q-2, R-4, S-1
(B) P-2, Q-3, R-1, S-4
(C) P-4, Q-1, R-2, S-3
(D) P-3, Q-4, R-2, S-1

Downloaded from www.pdf.tube

Oct/Nov 2009

**120.** Identify the incorrect statement regarding digital-only or neo-banks.
(A) They are totally immune to financial fraudsters due to absolute online security protocols.
(B) They offer financial services such as global payments and P2P transfers.
(C) They eliminate the need to visit brick-and-mortar branches.
(D) They build retail banking experiences from scratch in the virtual world.

Oct/Nov 2025

**121.** Identify the incorrect statement about Cloud Storage.
(A) It is usually provided by a commercial service provider.
(B) It offers a very good offsite backup unaffected by local disasters.
(C) It often requires an ongoing subscription fee for expanded space.
(D) It is typically faster than local backups because it bypasses internet connections.

May/June 2012

**122.** A small business uses a specialized file-level storage device built for local backups. The device houses several SATA hard drives plugged into a network router, providing easy file access to a heterogeneous group of computers. Which storage technology is the business utilizing?
(A) Storage Area Network (SAN)
(B) Flash Jump Drive
(C) Network Attached Storage (NAS)
(D) Active Directory

Oct/Nov 2018

**123.** Identify the incorrect statement concerning "Interest Processing" in the banking software.
(A) The system allows for a large number of variations of interest processing routines.
(B) Interest capitalization can occur at predefined intervals or on an 'anniversary' date.
(C) Banded tiered rates may be set by amount or time, but never a combination of both.
(D) The system allows for table selected and banded rates offset from a prime rate.

May/June 2007

**124.** In the context of database administration, a DBA has many responsibilities. Which of the following is NOT typically a DBA's task?
(A) Developing the HTML-based front-end for user browsers.
(B) Enrolling users and maintaining system security.
(C) Ensuring compliance with database vendor license agreements.
(D) Allocating system storage and planning future storage requirements.

Oct/Nov 2014

**125.** Identify the correct statement regarding the physical infrastructure of a Core Banking Solution.
(A) Branches hold high-capacity central servers, while the central hub has low-end computers.
(B) Branches have low-end computer servers connected to a high-capacity central server.
(C) The branch servers do not hold any local databases for intermediate transactions.
(D) Core banking systems rely solely on optical discs sent daily via mail.

www.nodia.in

NODIA

# ANSWERS

1. (D) P-1, Q-2, R-4, S-3
The correct configuration for an international banking system requires mapping multi-currency features to foreign exchange revaluation and multi-entity support to regional or subsidiary operations. Furthermore, multi-branch capabilities handle inter-location activities across time zones, while bulk transaction entry allows for real-time clearing processes. This specific combination ensures the system manages complex global commercial banking operations effectively and accurately.

2. (C) Branches can continue to function locally without hindrance during a breakdown of connectivity.
A 'store and forward' facility is a critical component in core banking environments designed to maintain business continuity. It allows local branches to process transactions even when the wide area network connection to the central server is lost. Data is stored locally and synchronized later, ensuring that customer services are not interrupted by technical connectivity failures during branch operations.

3. (C) Managing mutual funds, portfolios, and capital
Non-Banking Financial Institution software is categorized within the broader banking software ecosystem to handle specific financial products. Its primary role involves the comprehensive management of mutual funds, portfolio investments, and capital market activities. By using specialized modules, institutions can efficiently oversee wealth management services that differ from traditional retail banking functions like payroll processing or basic ledger reconciliation.

4. (C) Uses HTTP to serve files that form Web pages to users
A web server is a specialized software program designed to manage and deliver web content to users. It utilizes the Hypertext Transfer Protocol to process incoming requests and serve the necessary files that constitute web pages. This technology facilitates the communication between the user's browser and the backend systems, enabling the display of interactive online banking interfaces and resources.

5. (B) Implementation of fee variations strictly at the regional management level
Exception processing in banking software allows for necessary flexibility when applying fees and charges. However, claiming that fee variations are implemented strictly at the regional management level is incorrect because the system allows much more granular control. Variations can be applied based on specific products, account types, or individual transaction events, providing a versatile mechanism for managing diverse banking costs.

6. (B) Browser-based front-ends and back-end database legacy systems
In a standard data center architecture, the Application Server serves as a vital middle tier in the communication process. It acts as an intermediary layer that connects browser-based front-end interfaces used by customers or staff with the complex back-end database systems. This arrangement allows for the execution of business logic and efficient processing of data-heavy banking transactions across the network.

7. (B) RTGS
Reconciliation and settlement software is designed to manage the flow of funds and ensure accurate balances between different financial institutions. Real Time Gross Settlement systems are a prime example of this category, facilitating the continuous and instantaneous processing of high-value interbank transfers. These systems are essential for maintaining liquidity and minimizing the settlement risks associated with large-scale financial operations.

8. (B) (I), (III), and (IV)
Interest and base rate processing in modern banking systems offers significant flexibility through various configurations. Systems support table-selected and banded rates that can be

Click Here to Buy book on Amazon

adjusted relative to a prime rate. Furthermore, base rates and margins can be applied globally across all product categories or tailored individually for specific products, ensuring that the bank can respond dynamically to changing market conditions.

9. (B) Daily reports that increase administration and telephone costs
Centralized Money Management provides numerous operational advantages, such as fund consolidation for maximizing investments and increased banking flexibility through local branch deposits. However, generating daily reports that lead to higher administration and telephone costs is a significant drawback rather than a benefit. Effective systems aim to reduce these costs through automation and electronic reporting rather than increasing the manual burden.

10. (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Performance management utilities are essential for monitoring the capacity and scalability of a banking system. As transaction volumes grow and new financial products are introduced, it is vital to conduct benchmarks to maintain satisfactory response times for end-users. The assertion and reason are both true and directly related, as continuous monitoring ensures the infrastructure can handle expanding banking requirements effectively.

11. (D) JBoss
JBoss is a widely recognized open-source application server that originates from the JBoss community, now part of Red Hat. Unlike proprietary solutions from vendors like Oracle or IBM, it provides a flexible and community-driven platform for hosting complex enterprise applications. It is frequently used in banking environments to manage the middle-tier logic required for high-volume transaction processing and services.

12. (C) Relational database systems using standard codes stored in master tables
The core of an Integrated Banking System relies on a sophisticated relational database architecture. This system uses standard codes stored in master tables to manage diverse operational parameters like position, gaps, and asset-liability management. By utilizing these master tables instead of hard-coded instructions, the software gains flexibility and consistency, allowing for standardized processing across all banking modules and financial activities.

13. (A) Open system, multi-tier architecture for seamless integration
Modern centralized banking solutions are typically built on an open system, multi-tier architecture. This design facilitates seamless integration between various delivery channels and the core database, supporting high levels of scalability and flexibility. By separating the presentation, application, and data layers, banks can more easily upgrade individual components and maintain a robust infrastructure that adapts to evolving financial service requirements.

14. (C) Phone Pay/Bill Pay
Phone Pay or Bill Pay facilities provide customers with a convenient method to manage their finances remotely. By using a secure password and account number over the telephone, users can authorize the system to automatically generate cheques debited from their savings accounts. This automated service bridges the gap between traditional paper-based transactions and modern electronic banking, offering accessibility for various users.

15. (D) It is a free open source web server known for high performance and low resource usage.
Nginx is a highly efficient, free, and open-source web server recognized for its ability to handle large volumes of simultaneous connections with low resource consumption. Its event-driven architecture makes it superior to traditional thread-based servers in terms of memory usage and speed. Consequently, it is often favored for high-performance environments where stability and efficient delivery of web content are paramount.

16. (A) Time-consuming integration and inadequate level of support
Choosing to deploy multiple independent application software programs instead of a single integrated banking solution often leads to significant operational challenges. This approach

Downloaded from www.pdf.tube

(A) Because internet data cannot be converted into bytes for consumer usage
(B) Because ISPs are typically standardized to advertise using only bits to users
(C) Standardization of raw data transfer rates using the fundamental bit unit
(D) Because megabytes are exclusively reserved for tape cassette storage systems

**May/June 2017**

**101.** Identify the incorrect statement regarding the reporting features of an Integrated Banking System.
(A) The system restricts real-time inquiry on profiles to average balance maintained.
(B) There must be extensive reporting on both current and trend values within the system.
(C) Statistical summaries can be produced by currency, branch, area, and institution.
(D) There may be provision for generating Central Bank reports.

**Oct/Nov 2005**

**102.** Identify the incorrect statement regarding SAN storage.
(A) SAN storage is not highly scalable and relies entirely on single IDE enclosures.
(B) SANs provide block-level access to shared data storage.
(C) SAN storage provides synchronous replication which is a key requirement for disaster recovery.
(D) SAN environments are highly resilient, equipped with dual fabrics and highly available storage arrays.

**May/June 2020**

**103.** Standard regulatory frameworks for digital lending address several malpractices. Which of the following is NOT typically prohibited under these rules?
(A) Data scraping from consumer phones
(B) The use of physical branch networks by NBFCs
(C) Automated credit limit increases
(D) Lending activities operating without explicit upfront disclosure of costs

**Oct/Nov 2015**

**104.** Match the emerging technology in List I with its application in banking in List II:
List I: Technology
P. Artificial Intelligence
Q. Robo Advisors
R. Neo-banks
S. Bank-as-a-Service (BaaS)
List II: Application
1. Low-cost alternative to traditional investment advisors offering a broad range of services.
2. Automating middle office functions like risk assessment and credit underwriting.
3. Digital-only entities offering global payments and trading in various assets.
4. An end-to-end process enabling third-party organizations to connect via APIs.
(A) P-1, Q-2, R-4, S-3
(B) P-3, Q-4, R-1, S-2
(C) P-2, Q-3, R-1, S-4
(D) P-2, Q-1, R-3, S-4

**May/June 2013**

**105.** The following question consists of two statements: Assertion (A) and Reason (R). Choose the correct option based on these statements.
Assertion (A): In centralized banking, deposits made in any branch reflect immediately, allowing customers to withdraw money from any other branch.
Reason (R): All branches access applications from central servers or a data center, ensuring real-time synchronization of customer databases.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2021**

**106.** During an audit, it is found that multiple computers across different global branches of a bank are administered as a single unit, sharing common rules, username/password authentications, and managed by a central domain controller. This network configuration is a direct example of a:
(A) Standalone workgroup
(B) Windows Domain
(C) Peer-to-Peer torrent network

NODIA

driven approach helps banks improve customer engagement and optimize their marketing strategies.

**25.** (B) Push sweep
A push sweep facility is an automated banking tool that transfers funds from a primary account to another account once a specific balance threshold is reached. In this scenario, the customer instructs the bank to move any amount exceeding ₹50,000 into an investment account. This proactive movement of funds helps users maximize their interest earnings or meet specific investment goals automatically.

**26.** (D) Robust, expandable, and platform-isolated
The architecture of an Integrated Banking System is strategically designed to be robust, expandable, and platform-isolated. This means the system can grow to handle increased transaction volumes and integrate new technologies without being dependent on a specific hardware platform. Such design choices ensure long-term sustainability and the ability to adapt to the changing technological landscape within the global financial industry.

**27.** (A) P-3, Q-1, R-2, S-4
Web servers and containers serve distinct roles in hosting online services. The Apache Web Server is modular open-source software used widely across various machines, while Microsoft's IIS is a proprietary product that restricts custom module additions. Nginx utilizes a scalable event-driven architecture, and web containers specifically handle servlet requests within an application server. Matching these characteristics correctly identifies their operational differences.

**28.** (A) Multi-Entity support
Multi-entity support is a vital characteristic for international banks operating across different regions and continents. This capability allows a single central computer system to manage multiple distinct subsidiaries, each maintaining its own base currency and local reporting requirements. It enables the consolidation of general ledgers while respecting the legal and operational independence of various business units within a global banking organization.

**29.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Generating reports centrally is significantly more efficient than using distributed banking solutions. In a distributed model, consolidating financial statements from numerous isolated branch locations is a time-consuming and expensive process. Centralization allows for immediate data aggregation at a central server, enabling the rapid production of returns for regulatory bodies. Thus, the assertion and reason are both accurate and logically connected.

**30.** (D) Collateral Management System
A collateral management system is responsible for tracking and valuing assets used to secure loans. It ensures that collateral is pledged only up to its nominated value and can manage complex relationships where assets are linked across different entities. This system provides the necessary controls for global lending facilities, preventing the over-utilization of collateral and maintaining the bank's overall risk profile.

**31.** (C) P-2, Q-1, R-4, S-3
Storage devices are categorized based on their underlying technology. Magnetic storage includes traditional formats like floppy diskettes, while optical storage refers to laser-read media like Blu-ray discs. Flash memory, utilized in Solid State Drives, offers faster electronic data access. Finally, cloud storage services like Amazon S3 provide scalable offsite data management via the internet. Correctly identifying these examples illustrates technological diversity.

**32.** (B) P-4, Q-3, R-1, S-2
Several factors influence practical download speeds. Packet delivery methods introduce overhead through message headers, and server load can lead to connection throttling when requests are excessive. Routing involves finding the shortest path, which impacts latency based on distance. Finally, the Network Interface Controller on the client device represents a hardware limitation. Understanding these factors helps in diagnosing network performance and bandwidth issues.

Click Here to Buy book on Amazon

**33.** (B) Network Administrator
A network administrator is tasked with maintaining the integrity and security of a bank's communication infrastructure. Their responsibilities include testing the network for potential weaknesses, setting up email filters to prevent spam or phishing, and installing essential security programs. These actions are vital for protecting the bank's data from external threats and ensuring that internal communication channels remain operational.

**34.** (D) Multiply Megabits by 1024 to get Kilobits, then divide by 8 to get Kilobytes.
To calculate download speed in Kilobytes per second from a connection speed given in Megabits per second, a specific mathematical progression is required. First, multiply the Megabits by 1024 to convert the value into Kilobits. Then, divide the resulting figure by 8, since there are 8 bits in every byte. This process yields the theoretical maximum speed for file transfers.

**35.** (B) (I), (II), and (IV)
Network Attached Storage is a versatile storage solution that typically utilizes IDE or SATA hard drives in an array. It connects directly to a network through an Ethernet port on a router or hub and can be configured with RAID for enhanced reliability and performance. Unlike SAN systems, it does not require specialized Fiber Channel switches or complex switched fabric architectures.

**36.** (A) It operates as a banking correspondent and technology service provider to traditional banks.
In the Indian financial ecosystem, neo-banks operate primarily as technology service providers and banking correspondents in partnership with traditional banks. Because they lack a full banking license from the central bank, they cannot accept deposits or lend money on their own books. Instead, they leverage their digital platforms to offer a superior user experience while using the regulated infrastructure of partners.

**37.** (A) Building and maintaining the server and resolving helpdesk issues
An Application Administrator is primarily focused on the operational health of the software environment. Their duties include building and maintaining the server infrastructure, resolving helpdesk issues related to the application, and ensuring that users can access the system effectively. They bridge the gap between software development and end-user support, focusing on system uptime and the resolution of daily technical problems.

**38.** (D) The raw data transfer rate of the connection provided by the ISP.
Connection speed, often referred to as internet bandwidth, represents the raw data transfer rate of the link provided by an Internet Service Provider. It measures the capacity of the connection to move data between the ISP's network and the user's location. This metric is different from the actual download speed, which can be influenced by various internal and external factors.

**39.** (D) Download speed depends strictly on a single central client-server node.
Torrent downloading utilizes a peer-to-peer model where data is shared among all connected users, known as peers. This decentralized approach means that speed depends on the number of seeders uploading the file and the total swarm size. Unlike traditional downloads, it does not rely on a single central client-server node, allowing for more efficient distribution of large files across networks.

NODIA

**40.** (C) Both (I) and (II) are correct
Storage Area Networks are specialized, high-speed networks that provide block-level access to storage. They often use switched fabric architectures with Fiber Channel connectivity to ensure high performance. A key advantage of SAN is its support for synchronous replication, which is vital for disaster recovery strategies, allowing data to be mirrored instantly across different locations to ensure business continuity in emergencies.

**41.** (B) Niyo
Niyo is a prominent neo-bank that offers specialized financial products like the 2-in-1 digital savings account. This product is designed for modern users who want to earn high interest on their savings while also having access to zero-commission mutual fund investments. By integrating wealth management features directly into a mobile banking app, it provides a seamless and cost-effective digital experience.

# STUDYING FROM PDFs?

# THINK AGAIN.

If you are studying only from PDFs,
you are wasting valuable time.

Research shows that learning from

**PRINTED BOOKS** has up to

**4× HIGHER RETENTION**

than studying from screens.

**PRINT BOOK = BETTER MEMORY**

**PDF = LOWER RETENTION**

Those who study from **PRINTED BOOKS**
move **AHEAD.**

Others are left **BEHIND**
in competition.

In competitive exams,
being average is not enough.

## STAY ONE STEP AHEAD.

**42.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
A Windows domain enhances network security by centralizing authentication and management. When a domain is established, it can support a certification authority, which enables the use of smart cards and digital certificates for identity verification. This infrastructure allows users to utilize enhanced security for VPN connections and other remote access methods, making it an essential component for secure enterprise networking.

**43.** (B) 256 KBps
To find the theoretical maximum download speed for a 2 Mbps connection, you must convert Megabits to Kilobits and then to Kilobytes. Multiplying 2 by 1024 gives 2048 Kilobits. Dividing this result by 8, to account for the eight bits in a byte, equals 256 KBps. This calculation represents the limit under ideal conditions without any network overhead or throttling.

**44.** (D) Graphical design, attractiveness, and first impressions of personality
In the context of online banking website design, the "look" refers to the visual presentation and overall aesthetic appeal. This includes the graphic design, the use of colors, and the attractiveness of the interface, which together create a professional first impression. A well-designed site conveys the personality of the bank and builds trust, similar to the ambiance of physical branches.

**45.** (C) Fingerprint login and the ability to place temporary holds on cards
User surveys indicate that specific mobile banking features are highly valued for their convenience and security. Fingerprint login provides a fast and secure method for accessing accounts without typing passwords. Additionally, the ability to place temporary holds on cards offers users immediate control over their finances in case of loss or theft, significantly enhancing the overall user experience and safety.

**46.** (A) (I) and (II) only
A Database Administrator's role is focused on the management and optimization of the database environment. Key responsibilities include monitoring system performance to ensure efficient data retrieval and planning comprehensive backup and recovery strategies to protect information. While they may interact with various systems, providing technical support for wireless remote terminals is generally outside their specialized scope of database maintenance.

**47.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Download managers can enhance the speed of file transfers by establishing multiple parallel connections to a server. This technique allows different parts of a file to be downloaded simultaneously, maximizing the use of available bandwidth. The assertion that these tools improve speed and the reason explaining their use of parallel connections are both true and logically linked to network performance.

**48.** (B) NAS provides file-level access, whereas SAN provides block-level access
The fundamental difference between Network Attached Storage and Storage Area Networks lies in how they provide data access. NAS is designed for file-level access, making it suitable for sharing files across a local network via standard protocols. In contrast, SAN provides block-level access, allowing servers to treat the remote storage as if it were a local hard drive, which is more efficient for databases.

**49.** (A) A faster connection speed guarantees maximum download speed even if the local Disk Read/Write Speed is extremely slow.
Practical download speeds are influenced by several factors beyond the raw connection speed provided by an ISP. Background operating system services, server throttling, and packet overhead all play a role. Importantly, the claim that a fast connection guarantees maximum speed even with slow local disk read/write speeds is incorrect, as the storage device's performance can act as a significant bottleneck.

**50.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
A bank's internet presence offers unparalleled accessibility compared to a traditional brick-and-mortar location. Because a website can be visited by anyone with a computer and an

Downloaded from www.pdf.tube

It is incorrect to claim that the system restricts real-time inquiry solely to the average balance maintained, as modern systems offer comprehensive access to a wide range of profile data and transaction histories.

**102.** (A) SAN storage is not highly scalable and relies entirely on single IDE enclosures.
Storage Area Networks are known for being highly scalable and resilient, often featuring dual fabrics and available storage arrays for continuous operation. They provide block-level access and support synchronous replication for disaster recovery. Claiming that SAN storage is not scalable and depends entirely on single IDE enclosures is incorrect, as these characteristics describe much simpler and less capable storage solutions.

**103.** (B) The use of physical branch networks by NBFCs
Standard regulations for digital lending prohibit several malpractices, such as unauthorized data scraping and automated credit limit increases without consent. They also require full disclosure of costs to protect borrowers. However, the use of physical branch networks by Non-Banking Financial Companies is a traditional business practice and is not typically prohibited under rules specifically targeting digital lending activities.

**104.** (D) P-2, Q-1, R-3, S-4
Emerging technologies have specific applications in banking: AI automates middle-office functions, while Robo Advisors provide low-cost investment advice. Neo-banks offer digital-only financial services, and Bank-as-a-Service provides an API-based process for third-party integration. Matching these technologies to their roles demonstrates how they are transforming various aspects of the financial industry, from internal operations to customer-facing services.

**105.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
In centralized banking, all branches access applications from a central server or data center, ensuring real-time synchronization of the customer database. This allows deposits made at any location to reflect immediately across the entire system. Consequently, customers can withdraw money from any other branch without delay. Both the assertion and the reason accurately describe the seamless nature of centralized banking.

**106.** (B) Windows Domain
A network where multiple computers across different global branches are administered as a single unit with shared rules and central authentication is a Windows Domain. In this configuration, a central domain controller manages security policies and user access for all connected devices. This centralized management provides a consistent and secure operational environment for large organizations with multiple geographic locations.

NODIA

**107.** (A) Complex manual recovery procedures are no longer necessary.
High Availability Operation is a feature of modern banking systems that ensures near-automatic recovery from hardware failures. This means that complex and time-consuming manual recovery procedures are no longer required to restore services. By using fault-tolerant platforms and clustered processing, the system can maintain continuous operations even if a component fails, significantly reducing potential downtime for critical banking services.

**108.** (A) Network Interface Controller (NIC) limitations on the user's device
Practical download speeds can be reduced by external factors such as server capacity, packet delivery overhead, and routing distance. These are all related to the host or the network path. However, limitations from the Network Interface Controller on the user's device are considered internal, client-side hardware factors rather than external server-side or network-related influences on the transfer rate.

**109.** (D) Lack of licenses preventing them from accepting deposits on their own
Neo-banks often form strategic partnerships with traditional banks because they lack the necessary banking licenses to accept deposits on their own books. By collaborating with established, regulated institutions, neo-banks can offer financial services and manage customer funds while operating within the legal framework. This

**59.** (A) Only (I) is correct
File hosting websites often offer premium plans that remove common limitations such as speed caps and bandwidth restrictions placed on free users. While these plans allow for much faster downloads by utilizing more of the user's available bandwidth, they cannot exceed the maximum speed provided by the user's local ISP. Therefore, only the first statement regarding the removal of limitations is correct.

**60.** (B) Navigating between pages with links back to the main homepage
Successful online banking websites prioritize internal navigation to ensure a smooth user experience. This characteristic involves providing clear site maps, internal search engines, and consistent links that allow users to move between different sections and return to the main homepage easily. Good navigation prevents users from getting lost and ensures they can access various banking services efficiently without needing to use browser buttons.

**61.** (C) Appointment of a Nodal Grievance Officer to address customer grievances is made mandatory.
Regulatory guidelines for digital lending place a strong emphasis on protecting consumers from malpractice. A key requirement is the mandatory appointment of a Nodal Grievance Officer by regulated entities to address customer complaints. This ensures that borrowers have a dedicated and formal channel for resolving disputes, increasing accountability for digital lenders and providing a higher level of consumer protection in the industry.

**62.** (C) Assertion (A) is true, but Reason (R) is false.
Integrated Banking Systems use sophisticated validation techniques, such as password encryption and branch location checks, to secure user access. However, it is incorrect to assume that signing on automatically grants unconditional access to all functions. Access is typically conditional and restricted based on the user's specific role and authorization level, which helps prevent unauthorized actions and maintain strict internal financial controls.

**63.** (B) (III), (II), (I)
The Bank-as-a-Service process follows a logical chronological sequence. First, a Fintech startup pays a fee to access a BaaS platform. Following this, the established financial institution opens its API to the startup, allowing it to interact with the regulated banking infrastructure. Finally, the startup uses these APIs to build and launch its new financial applications and services for customers.

**64.** (A) (I), (II), (IV), and (V)
Regulatory bodies in India mandated that Urban Co-operative Banks and Regional Rural Banks implement core banking solutions to meet growing customer needs. A specific deadline of December 31, 2013, was set for UCBs to complete this transition. While this move was essential for modernization, it is generally accepted that both RRBs and UCBs met these requirements to improve their operational efficiency and services.

**65.** (C) Both (I) and (II) are correct
When selecting an IT vendor, banks consider various criteria such as accessibility and pricing options. Accessibility refers to how easily the vendor's services can be reached, often influenced by their local presence. Pricing options involve the vendor's flexibility regarding different contract types, such as fixed or variable pricing. Both factors are crucial for ensuring a stable and cost-effective partnership during system implementation.

**66.** (A) Application Server
An Application Server is the most suitable choice for hosting middle-tier business logic and managing complex transaction-based applications. It provides the necessary environment for running distributed application services and executing scheduled jobs. By acting as an intermediary between the user interface and the database, it ensures that business rules are applied consistently and that large volumes of transactions are processed efficiently.

**67.** (C) Neo Banks
Neo-banks are uniquely positioned to serve gig economy workers by using advanced technologies to provide fast, customized, and small-ticket financial products. Because they are digital-first and utilize modern data analytics, they can offer more flexible lending options without the need for physical branch visits. This agility allows them to

Click Here to Buy book on Amazon

internet connection, customers worldwide can access services at any time. This global reach and 24/7 availability confirm both the assertion and the reason, highlighting how digital platforms transcend the physical limitations of geography.

**51.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Neo-banks in many jurisdictions, including India, operate under a model where they cannot accept deposits or lend money on their own books. This is because they do not hold full banking licenses and must therefore partner with traditional banks or non-banking financial companies to provide regulated services. Both the assertion and the reason accurately describe this strategic and regulatory framework.

**52.** (D) Samba
Integrating non-Windows computers into a Windows-based domain environment requires specialized software to facilitate communication and authentication. Samba is a popular open-source software suite that provides seamless file and print services between different operating systems. It allows Linux or Unix-based machines to act as members of a Windows domain, making it a suitable tool for banks with diverse IT infrastructures.

**53.** (C) Storage Area Network (SAN)
For a bank requiring high resilience, scalability, and synchronous replication for block-level data, a Storage Area Network is the most appropriate solution. SANs are built for high-performance environments and provide the necessary infrastructure for clustered virtual servers and disaster recovery. Unlike simpler NAS or external drives, SANs offer the specialized connectivity and management features needed for mission-critical enterprise data storage.

**54.** (C) Seeder - A user who is uploading data into the network
In torrent networks, specific terms define the roles of users within the swarm. A seeder is a user who has a complete copy of the file and is actively uploading data to others. This role is essential for the health of the network, as it ensures that new users can download the data they need. Seeders differ from leechers, who are still downloading.

**55.** (A) Relationship where 8 bits equal 1 byte, making Kilobytes smaller
The difference between connection speed and download speed units is based on the fundamental relationship where 8 bits equal 1 byte. Internet Service Providers usually advertise bandwidth in Megabits per second, which is a bit-based measurement. However, file sizes and download rates are typically expressed in Bytes. This means a numerical value for connection speed will always be larger than the corresponding download speed.

**56.** (A) Group of computers administered as a unit with common rules
A domain is a group of computers and devices on a network that are administered as a single unit with common rules and procedures. Within a domain, a central server known as a domain controller manages user authentication and security policies. This structure allows for centralized management of resources and users, ensuring consistent security and easier administration across a large organizational network.

NODIA

**57.** (A) Quantum Computing
While Artificial Intelligence, Blockchain, and Robotic Process Automation are recognized as primary drivers of value chain disruption in FinTech, Quantum Computing is not yet considered a prominent driver in the same category. Although it holds potential for the future, current disruption is more heavily influenced by technologies that improve efficiency, security, and customer experience through automation and decentralized ledger systems.

**58.** (A) Vulnerability to local physical disasters such as theft and floods
Cloud storage offers several pros and cons for data management. Common disadvantages include high ongoing subscription costs and slower transfer rates compared to local storage. However, vulnerability to local physical disasters, such as floods or theft, is not a disadvantage of cloud storage; rather, its resistance to these local events is a major benefit, as data is stored in remote data centers.

and efficient memory management even when handling numerous simultaneous connections.

76. (C) (I) and (III) only
The Bank-as-a-Service model is characterized by established banks allowing Fintech startups to connect to their systems through APIs. This enables startups to launch innovative services using the bank's existing regulated infrastructure without needing to build their own heavy hardware environment from scratch. This collaborative approach fosters innovation in the financial sector while maintaining compliance with regulatory standards and banking security.

77. (D) POS and kiosk systems are considered basic elements of CBS.
Core Banking Solutions provide several key elements that enhance the customer experience, such as "anywhere banking" and integrated digital channels. Point of Sale terminals and kiosks are considered basic elements of a modern CBS, allowing users to conduct transactions conveniently outside traditional branch hours. These technologies ensure that banking services are more accessible and integrated into the customer's daily activities.

78. (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Timely regulation of Fintech is crucial for balancing innovation with enterprise safety. Acting too early could stifle new ideas, whereas waiting too long might allow harmful practices to become deeply rooted. Therefore, regulatory measures are designed to be implemented at a stage where they can prevent harm without restricting the creative growth of the financial technology sector, as stated in the text.

79. (B) Either individually by product type and category or globally
The Base Rate Processing system in a bank allows for the management of fundamental interest rates. Margins on these base rates can be applied flexibly, either individually based on specific product types and categories or globally across all banking products. This versatility allows the institution to tailor its interest rate strategy to different market segments while maintaining a centralized control mechanism.

80. (D) Multi-Currency operations
A banking system's multi-currency capability is demonstrated when it can instantly process foreign exchange transactions. The system automatically performs calculations in both the base currency and the foreign currency, extracting the necessary figures without requiring manual batch processing. This real-time functionality is essential for international operations, ensuring accurate and immediate updates to account balances during global trade and currency exchanges.

81. (C) Internet Control Message Protocol (ICMP)
Application servers use various methods to forward requests from a web server, such as Common Gateway Interface, Java Server Pages, and Active Server Pages. These technologies allow for the creation of dynamic web content. However, Internet Control Message Protocol is a network-layer protocol used for diagnostic and error messages, and it is not a method for forwarding application-level web requests.

82. (B) (I), (II), (III), and (V)
Digital lending regulations incorporate several measures to protect consumers, such as prohibiting data scraping from phones and requiring explicit consent for data collection. They also mandate upfront disclosure of all costs and provide a cooling-off period for borrowers. However, mandatory automated credit limit increases are not typically a part of these regulations, as they could lead to excessive consumer debt.

83. (D) Incumbency
When a bank prioritizes a vendor's prior history and their status as a "preferred vendor," it is evaluating the criterion of incumbency. This reflects the value placed on an existing relationship and the vendor's familiarity with the bank's internal processes and systems. Incumbency can simplify the transition to new architectures because the vendor already understands the organization's unique requirements.

84. (C) Immediate consolidation of statements at the central server
Consolidated returns and reporting are much more efficient in a centralized solution because all data is stored on a single central server. This

NODIA

allows for the immediate aggregation of financial statements across all branches, eliminating the need to physically collect and manually merge reports from distributed locations. Consequently, the bank can produce regulatory returns much faster and at a lower cost.

**85.** (C) Non-Customer External Debit Inquiries
The Inquiries module in banking software supports various information requests, such as short inquiries, advances history, and security document movements. These help staff and customers track account activities and asset status. However, "Non-Customer External Debit Inquiries" is not typically a standard inquiry type, as the system is primarily designed to manage and provide information related to the bank's own customers.

**86.** (B) Physical branch layout design
Artificial Intelligence significantly enhances various financial processes, including risk assessment, anti-fraud measures, and credit underwriting. These backend and middle-office operations benefit from AI's ability to analyze large datasets and identify patterns. Designing the physical layout of a brick-and-mortar branch is a traditional architectural task and is not among the primary financial processes currently transformed by AI in Fintech operations.

**87.** (B) P-3, Q-4, R-1, S-2
The interaction between web server components follows a specific flow: the Web Client sends an HTTP request, and the Static Data Store provides a response for static files. The Application Server houses the container and manages data store interactions, while the Web Container processes servlets and returns the response to the web server. Correctly matching these components illustrates the multi-tier architecture.

**88.** (B) Irrelevance of incumbency because banks always prefer new vendors for IT
Vendor selection for banking IT involves evaluating security standards, track records, and total costs. It is incorrect to suggest that incumbency is irrelevant. In fact, banks often value existing relationships with vendors who understand their systems. A vendor's prior performance and familiarity with the bank's infrastructure are important factors that can influence the decision-making process for new IT projects.

**89.** (B) Store and forward facility
The store and forward facility is specifically designed to handle network interruptions in a core banking environment. When a wide area network failure occurs, branch servers continue to process and store transactions locally. Once connectivity is restored, these intermediate transactions are automatically synchronized with the central database. This ensures that banking operations can continue smoothly without being entirely dependent on constant connectivity.

**90.** (A) In different master tables (e.g., Position, gaps, ALM codes)
Integrated Banking Systems use standard codes to ensure consistency across various modules. These codes, which define parameters for asset-liability management, position tracking, and other financial functions, are typically stored in centralized master tables. By maintaining these codes in a structured relational database, the system can provide uniform processing and reporting throughout the entire institution, rather than relying on isolated files.

**91.** (B) Internal navigation
Internal navigation on a website is enhanced by features like site maps, internal search engines, and consistent links back to the main page. These tools help users find information efficiently and move between pages without getting lost. For a bank's website, good navigation is essential for ensuring that customers can easily access various online services and complete tasks without frustration.

**92.** (C) Banking IT Knowledge
When a bank assesses a vendor's understanding of the transition from legacy systems to distributed architectures, it is evaluating the vendor's banking IT knowledge. This criterion focuses on the vendor's technical expertise in specific areas of financial technology, such as data center consolidation and groupware. Having a partner with deep IT knowledge is crucial for successfully implementing complex modern banking infrastructures.

Downloaded from www.pdf.tube

**93.** (C) Flash memory became cheaper, faster, and more reliable than magnetic media
Flash memory has become the preferred storage medium over magnetic media because it has become cheaper, faster, and more reliable. Unlike traditional hard drives that use moving parts and magnetic fields, flash memory uses electronic circuits, which increases durability and data access speeds. This technological shift has led to the widespread adoption of Solid State Drives in modern computing systems.

**94.** (C) There should be no impact upon on-line response times to end users
A key requirement for a 'store and forward' facility is that there should be no impact on online response times for end-users while the system is in local processing mode. This ensures that even during a network outage, customers and staff do not experience delays in transaction processing. Maintaining high performance during these periods is essential for consistent and reliable banking operations.

**95.** (B) Most mobile users research bank app capabilities before opening accounts
Recent global studies on Fintech usage show that most mobile users are proactive in researching a bank's app capabilities before they decide to open an account. This behavior highlights the importance of digital features and a user-friendly interface as competitive advantages for modern banks. Customers now view mobile app functionality as a primary factor in their choice of financial service provider.

**96.** (B) P-3, Q-4, R-1, S-2
Banking software types are matched to specific modules: core banking handles deposits and advances, while MIS software manages asset-liability and non-performing assets. Reconciliation and settlement software is used for systems like the Electronic Clearance System, and NBFI software deals with refinance management. This categorization helps in understanding the different functional areas within a comprehensive integrated banking software environment.

**97.** (B) (I), (III), and (IV)
An Application Administrator's standard responsibilities include technical tasks such as generating reports using scripts, maintaining metadata, and supporting document management facilities. They also provide essential technical support to web designers to ensure the software environment is stable. Designing the physical layout of brick-and-mortar branches is an architectural and facilities management role, not a function of the Application Administrator.

**98.** (A) (I), (II), (III), and (IV)
Artificial Intelligence is expected to significantly impact financial institutions by helping combat cybercrime, utilizing chatbots for support, and optimizing middle-office processes like anti-fraud. These advancements lead to improved cost-effectiveness and operational efficiency. However, the idea that AI will completely eradicate the need for all human employees in the near future is an exaggeration and not a standard industry expectation.

**99.** (B) It measures the geographical proximity of the vendor's local service office.
The "Technical Skills" criterion in vendor selection focuses on the vendor's proficiency with specific software tools, techniques, and programs required for the project. It evaluates the expertise the vendor possesses regarding the necessary products. Measuring the geographical proximity of the vendor's local service office is actually a factor of "Accessibility" rather than a measure of their technical software capabilities.

NODIA

**100.** (C) Standardization of raw data transfer rates using the fundamental bit unit
Connection speed is usually measured in Megabits per second because it represents a raw data transfer rate, which is standardized using the fundamental bit unit. Internet Service Providers use this standard for advertising and technical specifications. While download speeds are often viewed in Bytes by users, the underlying bit-based measurement remains the industry standard for defining the capacity of communication links.

**101.** (A) The system restricts real-time inquiry on profiles to average balance maintained.
Integrated Banking Systems provide extensive reporting capabilities, including current values, trend analyses, and statistical summaries by currency or branch. These reports are essential for management and regulatory compliance.

meet the specific needs of modern workers who require quick financial solutions.

**68.** (D) (I), (II), (III), and (IV)
Effective international deployment of a banking system requires the integration of diverse components including retail, e-commerce, treasury, trade, and management information systems. These modules allow the bank to handle a wide range of global financial activities, from consumer banking to complex international trade finance and high-level management reporting. Having all these integrated ensures the bank can operate efficiently across different markets.

**69.** (D) (I), (II), and (III)
Centralized banking solutions support multiple delivery channels to provide customers with convenient access to their accounts. Standard channels include Automated Teller Machines for cash services, mobile banking for on-the-go management, and tele-banking for assistance over the phone. These channels are integrated with the central database, ensuring that all transactions are reflected in real-time across the entire banking system for the user.

**70.** (C) P-3, Q-4, R-1, S-2
Vendor selection involves evaluating industry knowledge, banking IT knowledge, application familiarity, and project management skills. Industry knowledge focuses on understanding regulations and competition, while banking IT knowledge covers technical architectures like distributed systems. Application familiarity refers to expertise in specific vendor software, and project management relates to handling budgets and schedules. Matching these criteria correctly ensures the bank chooses a capable partner.

**71.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
A Database Administrator must stay informed about emerging technologies and new design approaches to manage complex database environments effectively. Their responsibilities include capacity planning, installation, security, and making structural modifications based on developer requirements. Both the assertion and the reason are true and related, as staying updated is necessary for performing these technical tasks in a rapidly changing technological landscape.

**72.** (B) Robotic investment technology providing broad services with minimum investment
Robo Advisory refers to the use of automated, algorithm-driven technology to provide investment services with minimal human intervention. These platforms offer a broad range of investment advice and portfolio management at a lower cost than traditional advisors, making them accessible to a wider audience. This technology allows users to manage their investments efficiently using digital tools while requiring smaller initial investments.

**73.** (D) Sweeps - Manages collateral assignment against global facilities
Integrated Banking Systems include various modules like Phone Pay for automatic cheque generation and Inquiries for handling account details. Fees and Charges modules support tiered structures for transaction values. However, the claim that Sweeps manages collateral assignment is incorrect. Sweeps are used for automated balance transfers between accounts, while collateral management is handled by a dedicated system for tracking assets and security documents.

**74.** (C) Mainframe Tape Drive
The Communications Interface System in a banking architecture connects the core system to various external delivery channels and networks. These typically include SWIFT for international transfers, ATMs for cash transactions, and call centers for customer service. A mainframe tape drive, however, is considered an internal peripheral for data storage rather than an external communication interface used for customer-facing or interbank services.

**75.** (D) Nginx uses threads to handle requests, resulting in highly unpredictable memory usage.
Web servers like Apache and Microsoft's IIS are fundamental for hosting online services, each with unique modularity and security characteristics. It is incorrect to state that Nginx uses threads to handle requests resulting in unpredictable memory usage. In fact, Nginx is known for its event-driven, non-threaded architecture, which provides highly predictable

Click Here to Buy book on Amazon

allows them to focus on providing a superior digital experience while the partner handles banking responsibilities.

**110.** (C) Bank-as-a-Service (BaaS)
Bank-as-a-Service is an operational model where a Fintech company pays an established bank to access its regulated platform via APIs. This allows the startup to launch new financial products without needing to obtain its own banking license or build extensive infrastructure. It is a collaborative strategy that leverages the bank's established systems to bring new digital services to market.

**111.** (D) Each processing entity has an ID structure that is unique and separate from any part of the account or customer ID structure.
In a commercial banking system, "Multi-Branch" support requires that each processing entity has a unique ID structure. Importantly, this ID must be separate from any part of the account or customer ID structure to ensure proper tracking of inter-location activities. This design allows the system to manage transactions across different locations and time zones accurately while maintaining data integrity.

**112.** (C) Both (I) and (II) are correct
The "feel" of a website relates to how easily users can navigate between sections and efficiently complete online forms. Customers expect a professional and attractive digital environment that matches the safety and reputation of a physical bank. Both statements are correct, as they highlight the importance of both user experience and visual presentation in creating a successful online banking platform.

**113.** (B) (I) and (III) only
Torrent downloads replace the traditional client-server model with a peer-to-peer approach, where numerous parallel connections are used to download data parts simultaneously. While seeders upload complete files, leechers are users who are still downloading data. Correctly identifying that torrents use P2P and multiple connections explains why this method can be highly efficient for distributing large files across a network.

**114.** (A) (I), (II), and (III)
Setting up exception processing for fees and charges involves using specific parameters like the account type, interest category, and transaction level. These allow the system to apply variations in charges based on the nature of the transaction or the customer's profile. Irrelevant physical characteristics, such as a customer's height, are not used as parameters in these financial processing systems.

**115.** (B) (II), (III), (I)
Calculating download speed from connection speed follows a specific chronological sequence. First, identify the connection speed in Megabits. Next, multiply that value by 1024 to convert Megabits into Kilobits. Finally, divide the result by 8 to convert the Kilobits into Kilobytes per second. This sequence provides the correct mathematical transformation needed to understand the practical rate of data transfer.

**116.** (D) P-2, Q-3, R-1, S-4
Storage network terms are defined by their specific features: NAS provides file-level access via a router, while SAN offers block-level access using switched fabrics. Cloud storage acts as a scalable offsite backup accessed through the internet, and RAID configurations provide redundancy to increase reliability and performance. Correctly matching these terms helps in selecting the appropriate storage architecture for different needs.

**117.** (A) (I), (II), and (III)
A bank's administration software is typically responsible for managing internal organizational functions such as payroll, personal information systems, pension plans, and provident funds. These modules handle employee-related data and financial benefits rather than customer-facing banking transactions. Inter Branch Reconciliation is a core accounting function and is generally managed within the main banking or general ledger software instead of administration.

**118.** (D) Speed caps imposed by the server on regular, non-premium user accounts
When a user with a high-speed internet plan experiences slow downloads from a file hosting site while using a free account, the primary cause is often server-side throttling. File hosting

NODIA

**Oct/Nov 2019**

**20.** Identify the incorrect statement regarding the Positive Pay System.
(A) Customers must physically visit the branch to re-confirm cheque details without exception.
(B) The system involves the drawer re-confirming key details of the issued cheque to the bank.
(C) The system is typically applicable to various cheque payments that are valued beyond 50,000.
(D) If the issuer fails to inform the bank prior to presentation, the cheque will likely bounce.

**May/June 2009**

**21.** A central bank in a G-10 country wishes to implement a large-value funds transfer system that eliminates systemic interbank settlement risks by settling transactions continuously on a transaction-by-transaction basis in central bank money. The system that directly fulfills this mandate is:
(A) Multilateral Net Settlement System
(B) Bilateral Delayed Settlement System
(C) Real Time Gross Settlement (RTGS) System
(D) Batch-processed Electronic Clearing System

**Oct/Nov 2011**

**22.** Which of the following is the primary objective of implementing a Cheque Truncation System (CTS)?
(A) To eliminate the electronic transmission of magnetic ink data while maintaining physical exchange networks.
(B) To move electronic images instead of physical instruments, reducing payment time and transit costs.
(C) To enforce physical delivery of cheques to the drawee bank while utilizing digital tracking for final payment.
(D) To ensure that customers strictly use high-value cheques for all interbank transactions to improve security.

**May/June 2010**

**23.** A customer frequently issues high-value cheques to suppliers. The customer is advised by the bank manager to utilize a system that involves re-confirming key details of the cheque before it is processed in clearing. If the customer issues a cheque for 5,50,000 and fails to inform the bank prior to its presentation, the cheque bounces. Which system mandates this procedure?
(A) National Automated Clearing House
(B) Real Time Gross Settlement
(C) Structured Financial Messaging System
(D) Positive Pay System

**Oct/Nov 2024**

**24.** A gas service provider struggles with the high cost of printing, dispatching bills, and following up on late payments from thousands of users. To resolve this, they obtain an upfront mandate from their customers to pull the required bill amounts directly from their bank accounts on the due dates. This operational model exemplifies:
(A) Structured Financial Messaging System
(B) Credit Clearing System
(C) Cheque Truncation System
(D) Debit Clearing System

**May/June 2017**

**25.** All of the following are stated benefits of the Cheque Truncation System (CTS) for banks and customers, except:
(A) Superior verification and reconciliation processes for all clearing operations.
(B) Increased collection charges for cheques drawn on a bank within the grid.
(C) Operational efficiency for both banking institutions and their respective customers.
(D) Reduction of manual tasks which directly leads to a significant decrease in errors.

**Oct/Nov 2005**

**26.** Identify the correct breakdown of the 9-digit center code printed on a cheque.
(A) First three digits represent the branch, next three represent the bank, last three represent the city.
(B) First three digits represent the bank, next three represent the city, last three represent the branch.
(C) First three digits represent the city, next three represent the branch, last three represent the bank.
(D) First three digits represent the city, next three represent the bank, last three represent the branch.

Downloaded from www.pdf.tube

# CHAPTER 10

# Electronic Clearing and Settlement Systems

May/June 2016

**1.** Which of the following conditions is an exception to the required physical specifications for a cheque to be processed successfully?
(A) The cheque must have two white bands, one on the top and another on the bottom of the instrument.
(B) The white bands must contain encoding written in special magnetic ink.
(C) The bands should be free from any marking or impressions that could interfere with high-speed processing.
(D) The cheque can contain minor folds and minimal tabs on either end to assist automated sorting.

Oct/Nov 2009

**2.** Consider the following statements regarding the characteristics of a Debit Clearing System:
I It requires the service provider to obtain an authorization from the customer to debit their bank account.
II It is utilized primarily for regular and periodic payments to utility service providers.
III The service provider submits the letter of authority to the banker, who passes the debits to the respective branches.
IV The customer is heavily reliant on printing out bills and tracking due dates manually.
Which of the above statement(s) is/are correct?
(A) Only (I), (II), and (III)
(B) Only (I), (III), and (IV)
(C) Only (II), (III), and (IV)
(D) (I), (II), (III), and (IV)

May/June 2023

**3.** Which underlying feature makes Optical Character Recognition (OCR) an advanced technology compared to Magnetic Ink Character Recognition (MICR) in cheque processing?
(A) It relies on a specialized magnetic toner to identify character patterns.
(B) It utilizes an automated reader cum sorter to move physical cheques at high speeds.
(C) It eliminates manual encoding by capturing cheque images directly.
(D) It transmits digitized data exclusively through dedicated physical magnetic storage.

Oct/Nov 2018

**4.** An interbank funds transfer system where both processing and final settlement of funds transfer instructions take place continuously without netting debits against credits is defined as:
(A) Deferred Net Settlement System
(B) End-of-day Gross Settlement System
(C) Real Time Gross Settlement System
(D) National Electronic Fund Transfer System

May/June 2007

**5.** Consider the following statements regarding the benefits of the Cheque Truncation System (CTS):
I It provides a shorter clearing cycle, enabling technically possible realization of proceeds within the same day.
II It imposes strict geographical restrictions on jurisdiction to enhance verification processes.
III It reduces operational risk by securing the transmission route and centralized image archival.
Which of the above statement(s) is/are correct?
(A) Only (I) and (II)
(B) Only (I) and (III)
(C) Only (II) and (III)
(D) (I), (II), and (III)

Oct/Nov 2025

**6.** Identify the incorrect statement regarding Designated-time Net Settlement (DNS) systems.
(A) A participating bank's net position is

NODIA

May/June 2007

**47.** An individual who does not possess a bank account visits an NEFT-enabled branch and wants to transfer 65,000 in cash to a landlord's account to pay rent. The branch teller informs the individual that the transaction cannot be processed as requested. The most appropriate solution to facilitate the payment via NEFT is:
(A) To split the amount and send two separate cash-based NEFT transactions of 32,500 each.
(B) To open an account or use an existing account, as cash-based NEFT transfers are capped at 50,000.
(C) To use the RTGS system instead, depositing the cash directly into the clearing center.
(D) To demand the transaction be routed through the Indo-Nepal Remittance Facility.

Oct/Nov 2025

**48.** A banking consortium upgrades its existing deferred net settlement software. To save development costs, they modify the system so that each bank's internal processing gateway holds the full payment message, sending only a subset request to the central bank. The full message moves bilaterally to the receiver only upon settlement confirmation. This architecture represents the:
(A) V-shaped structure
(B) L-shaped structure
(C) Y-shaped structure
(D) T-shaped structure

May/June 2012

**49.** The Indian Financial System Code (IFSC) is an alpha-numeric code used by electronic fund transfer systems. How many digits does it contain?
(A) 9 digits
(B) 11 digits
(C) 13 digits
(D) 15 digits

Oct/Nov 2014

**50.** Which of the following is not one of the access options provided to participants in the new ISO 20022 compliant RTGS system?
(A) The Thick-client interface
(B) Web-API through the INFINET
(C) USSD *99# dial-in interface
(D) The Payment Originator module

May/June 2019

**51.** Arrange the following steps of an NEFT transaction in the correct chronological order:
I. The Clearing Centre sorts transactions destination bank-wise and prepares accounting entries.
II. The originating bank branch prepares and sends the message to its pooling centre.
III. The destination bank receives inward remittance messages and passes the credit.
IV. The pooling centre forwards the message to the NEFT Clearing Centre.
(A) II, IV, I, III
(B) I, II, III, IV
(C) II, I, IV, III
(D) IV, II, I, III

Oct/Nov 2006

**52.** Conceptually, why was the L-shaped message flow structure chosen for the CHAPS system over other architectures?
(A) Because it required a complete rewriting of the software supporting the previous DNS arrangement.
(B) Because it mandates that all payment routing is heavily centralized through the central bank's mainframe.
(C) Because it is the only structure compatible with the S.W.I.F.T. network protocols.
(D) Because it could be implemented by modifying rather than rewriting the existing DNS software arrangement.

May/June 2021

**53.** In the context of the interrelationship between RTGS and a Securities Settlement System (SSS), a real-time Delivery Versus Payment (DVP) system requires:
(A) Net settlement of funds at the end of the day, while securities settle continuously.
(B) A bilateral DNS agreement that delays securities transfer until the next processing day.
(C) Simultaneous final transfers of both securities and funds on a trade-by-trade basis.
(D) That both securities and funds legs are netted multilaterally before execution.

Oct/Nov 2010

**54.** A Nepali citizen working in India wishes to send money to a relative in Nepal who does not hold a

Click Here to Buy book on Amazon

credit.
(D) The payee branch processes the payments on the next day and all returns are submitted in the next day clearing.

**May/June 2005**

**13.** A business issues a cheque of 6,00,000 to a vendor. Despite the account having sufficient funds, the payee's bank returns the cheque unpaid. The drawer bank cites non-compliance with a mandatory confirmation rule introduced from January 1, 2021. This return is most likely attributed to the failure of the drawer to utilize:
(A) The Positive Pay System
(B) The Cheque Truncation System
(C) The National Financial Switch
(D) The Bharat Bill Payment System

**Oct/Nov 2022**

**14.** Which of the following best defines the process of Cheque Truncation?
(A) Printing details of the cheque using special magnetic ink on a designated physical band at the branch.
(B) Physically collecting all interbank cheques for manual exchange at a centralized clearing node.
(C) Stopping the physical cheque flow to the drawee and replacing it with electronic images and data.
(D) Encrypting the customer's account balance digitally to prevent unauthorized physical withdrawals from accounts.

**May/June 2018**

**15.** Identify the correct statement regarding gross settlement systems.
(A) The settlement of funds occurs on a net basis according to the system's rules.
(B) Settlement positions are calculated multilaterally as the sum of all transfers received minus those sent.
(C) Settlement takes place exclusively at the end of the processing day.
(D) Settlement of funds occurs on a transaction-by-transaction basis without netting.

**Oct/Nov 2016**

**16.** In the encoding details of the lower white band of a cheque, the center code comprises how many digits?
(A) 9 digits
(B) 6 digits
(C) 11 digits
(D) 13 digits

**May/June 2014**

**17.** Consider the following statements regarding Credit Clearing advantages:
I The company is saved from printing a large number of dividend warrants for small amounts.
II Customers must personally submit electronic warrants at the bank to receive the credit.
Which of the above statement(s) is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**Oct/Nov 2007**

**18.** Consider the following statements regarding the encoded details on a cheque:
I The transaction code is a 2-character field indicating the type of account, such as 10 for Savings and 11 for Current accounts.
II The final 13 digits in the lower white band represent the cheque number and center code combined.
Which of the statements is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**May/June 2025**

**19.** Which conceptual distinction accurately separates a Debit Clearing System from a Credit Clearing System?
(A) Debit clearing handles dividend disbursements, whereas credit clearing manages utility bill collections.
(B) Debit clearing requires physical cheques for every transaction, whereas credit clearing operates exclusively on magnetic tapes.
(C) Debit clearing requires RTGS mechanisms, whereas credit clearing utilizes only NEFT batches.
(D) Debit clearing pulls funds from customers' accounts periodically for utilities, whereas credit clearing distributes funds like dividends to multiple beneficiaries.

Downloaded from www.pdf.tube

calculated as the total value received minus total value sent.
(B) Large-value DNS systems are incompatible with the transmission and processing of payment messages in real time.
(C) DNS systems can be based on either bilateral or multilateral net positions.
(D) In end-of-day DNS, final settlement occurs only once at the end of the processing day.

**May/June 2012**

**7.** A common service provided in metropolitan and smaller cities for the benefit of banks to settle interbank cheques drawn on one another is known as a:
(A) Truncation Center
(B) Clearing House
(C) Central Processing Hub
(D) Magnetic Ink Node

**Oct/Nov 2014**

**8.** What is the primary purpose of banks making the Positive Pay System mandatory for high-value cheques?
(A) To generate higher fee income from corporate clients.
(B) To enhance the safety of cheque-based transactions and prevent fraud.
(C) To slow down the clearing process for high-value amounts.
(D) To ensure that customers maintain a minimum balance of 5,00,000.

**May/June 2019**

**9.** Match the attributes in List I to the corresponding clearing system in List II.
List I: (Service/Attribute)
P. Periodic payment for telephones, electricity, and gas
Q. Periodical dividend or interest payments
R. Saves cost on printing and couriering utility bills
S. Saves the task of reconciling paid and outstanding interest warrants
List II: (Clearing System)
1. Debit Clearing System
2. Credit Clearing System
3. Debit Clearing System
4. Credit Clearing System
(A) P-2, Q-1, R-4, S-3
(B) P-1, Q-2, R-3, S-4
(C) P-3, Q-4, R-1, S-2
(D) P-4, Q-3, R-2, S-1

**Oct/Nov 2006**

**10.** Match the encoded fields of a cheque in List I with their corresponding formats in List II.
List I: (Encoded Fields)
P. Cheque number
Q. Center code
R. Transaction code
S. Amount
List II: (Format)
1. 2-character field
2. 6-digit code
3. 13 digits
4. 9-field character
(A) P-4, Q-2, R-3, S-1
(B) P-2, Q-4, R-3, S-1
(C) P-2, Q-4, R-1, S-3
(D) P-3, Q-1, R-4, S-2

**May/June 2021**

**11.** The following question consists of two statements, an Assertion (A) and a Reason (R). Choose the correct option to describe the relationship between them.
Assertion (A): By definition, netting involves the accumulation of a number of transactions so that credits can be netted against debits.
Reason (R): Netting is perfectly compatible with genuinely continuous settlement in a real-time gross settlement environment.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2010**

**12.** Identify the incorrect statement regarding the processing of MICR cheques.
(A) The encoder is a machine used to write the details of the cheques in the lower band using magnetic ink.
(B) The cheque reader cum sorter is installed at the clearing house to process cheques at high speed.
(C) All MICR cheques presented during the day are strictly processed manually during regular banking hours to ensure immediate

NODIA

**May/June 2020**

**27.** Systems in which final settlement occurs at one or more discrete, pre-specified settlement times during the processing day are classified as:
(A) Designated-time settlement systems
(B) Continuous settlement systems
(C) Real-time settlement systems
(D) Unspecified gross settlement systems

**Oct/Nov 2015**

**28.** The following question consists of two statements, an Assertion (A) and a Reason (R). Choose the correct option to describe the relationship between them.
Assertion (A): Cheque truncation eliminates the need to move physical instruments across branches, except in exceptional circumstances.
Reason (R): The physical instrument is truncated at some point en-route to the drawee branch, and an electronic image along with MICR fields is transmitted electronically.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2013**

**29.** For which of the following scenarios is a Credit Clearing System most appropriate?
(A) A company collecting monthly post-paid bills from 10,000 customers.
(B) A retail customer transferring 5,00,000 for a specific real estate purchase.
(C) A listed company disbursing annual dividends to 50,000 investors.
(D) A toll plaza collecting vehicle transit fees automatically from passing cars.

**Oct/Nov 2021**

**30.** Identify the correct statement regarding CTS-2010 compliant cheques.
(A) They are processed solely using optical character recognition without any magnetic ink data.
(B) They are cleared on a real-time gross settlement basis immediately upon presentation.
(C) They are mandatory only for cheques drawn on banks located outside the grid.
(D) They are image friendly and possess enhanced security features.

**May/June 2024**

**31.** Identify the incorrect statement regarding the central entity's role in message delivery for RTGS structures.
(A) V-shaped structure — Central bank acts as the central entity for routing messages.
(B) Y-shaped structure — Central processor acts as the central entity for routing messages.
(C) V-shaped structure — Network operator independently handles all message routing without the central bank.
(D) L-shaped structure — Gateway bilateral exchange negates the need for a central message delivery entity.

**Oct/Nov 2008**

**32.** A firm needs to urgently remit 25,0,000 to a supplier. The payment must reach the beneficiary instantaneously and on a gross settlement basis, without waiting for the next clearing batch. Which system should the firm explicitly instruct their bank to use?
(A) NEFT
(B) RTGS
(C) IMPS
(D) SFMS Credit Clearing

**May/June 2006**

**33.** In the context of RTGS message flow structures, which of the following is the defining characteristic of a V-shaped structure?
(A) The sending bank directly transmits the full message to the receiving bank, bypassing the central bank's hub.
(B) The full message is passed to the central bank and sent to the receiver after settlement.
(C) Only a subset of settlement information is sent to the central bank, while a central processor holds the full message.
(D) The payment message is held at a system gateway until the central bank sends a finalized settlement confirmation.

**Oct/Nov 2017**

**34.** Match the components of the IFSC code in List I to their designated characters in List II.
List I: (IFSC Component)
P. Total length of the code

Click Here to Buy book on Amazon

providers frequently impose speed caps on non-premium accounts to encourage users to purchase paid subscriptions. These intentional limitations override the user's available bandwidth, resulting in a significantly slower transfer rate.

**119.** (A) P-3, Q-2, R-4, S-1
Neo-bank products often feature innovative tools like Niyo's zero forex markup and high interest rates. Other features include tools for investing spare change, voice-enabled finance tracking, and small-ticket credit products tailored for gig economy workers. Matching these products with their specific applications shows how neo-banks use technology to create specialized financial experiences that appeal to tech-savvy millennials and workers.

**120.** (A) They are totally immune to financial fraudsters due to absolute online security protocols.
Neo-banks offer various virtual financial services, such as global payments and P2P transfers, which eliminate the need for physical branches. However, it is incorrect to state that they are totally immune to financial fraudsters. No digital system can offer absolute security, and neo-banks must constantly update their security protocols to protect against evolving cyber threats and sophisticated fraudulent activities.

**121.** (D) It is typically faster than local backups because it bypasses internet connections.
Cloud storage provides a valuable offsite backup solution that is protected from local disasters and is typically managed by a commercial provider. While it offers expanded space through subscription fees, it is generally slower than local backups because data transfer is limited by internet connection speeds. Claiming that it is typically faster than local backups by bypassing the internet is incorrect.

**122.** (C) Network Attached Storage (NAS)
A business using a file-level storage device with SATA drives plugged into a network router is utilizing Network Attached Storage. This technology provides an easy way for multiple computers on a local network to access shared files. NAS is a cost-effective solution for local backups and file sharing, differing from the more complex block-level storage provided by Storage Area Networks.

**123.** (C) Banded tiered rates may be set by amount or time, but never a combination of both.
Modern banking software offers significant flexibility in interest processing, allowing for variations in capitalization intervals and routines. The system supports table-selected and banded rates offset from a prime rate. It is incorrect to claim that banded tiered rates cannot be set by a combination of both amount and time, as many financial products require such complex configurations for interest.

NODIA

**124.** (A) Developing the HTML-based front-end for user browsers.
A Database Administrator's role involves managing system storage, ensuring security, and maintaining compliance with vendor licenses. They are also responsible for modifying database structures based on developer needs. However, developing the HTML-based front-end for user browsers is not a DBA task; it is typically the responsibility of web developers or front-end engineers who focus on the user interface.

**125.** (B) Branches have low-end computer servers connected to a high-capacity central server.
The physical infrastructure of a Core Banking Solution is designed with low-end computer servers at the branch locations, which are connected to a high-capacity central server. This centralized model ensures that data is processed and stored primarily at the central hub while allowing branches to handle local tasks. This arrangement supports real-time synchronization and efficient data management across the entire bank.

Assertion (A): In RTGS systems, queues are most commonly generated when sending banks do not have sufficient covering funds in their central bank account.
Reason (R): Queuing is an arrangement designed to prevent limits from being breached or to manage liquidity more generally.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2022**

**41.** Identify the correct pair mapping the payment system to its fundamental settlement characteristic.
(A) RTGS — Settles in 48 half-hourly batches.
(B) NEFT — Facilitates one-to-one funds transfer occurring in batches.
(C) NEFT — Real-Time as well as Gross Settlement system.
(D) IMPS — Exclusively batch processing deferred to the next business day.

**Oct/Nov 2023**

**42.** Identify the incorrect statement concerning the Y-shaped message flow structure.
(A) The payment message is transmitted by the sending bank to a central processor.
(B) The central processor routes only a core subset of information necessary for settlement to the central bank.
(C) The full business information exchanged between sending and receiving banks is fully known to the settlement agent.
(D) Once settled, the full message containing confirmation is rebuilt by the central processor and sent to the receiving bank.

**May/June 2016**

**43.** Identify the incorrect statement regarding the charges and administration of RTGS.
(A) The Reserve Bank of India operates RTGS as a critical Financial Market Infrastructure.
(B) If banks choose to levy charges for RTGS transactions, RBI has set the cap at Rs 500 for each transaction.
(C) With effect from July 01, 2019, the Reserve Bank has waived the processing charges levied by it for RTGS transactions.
(D) The minimum amount to be remitted through RTGS is 2,00,000 with no upper ceiling.

**Oct/Nov 2009**

**44.** Consider the following statements regarding the NG RTGS system:
I It features a gridlock resolution mechanism and hybrid settlement facility.
II It lacks the capability to process multi-currency transactions.
III It provides access options like thick-client, Web-API, and Payment Originator module.
IV Participants can decide their mode of participation based on transaction volume and infrastructure cost.
V The system allows acceptance of future value dated transactions.
Which of the above statement(s) is/are correct?
(A) Only (I), (III), (IV), and (V)
(B) Only (I), (II), (III), and (IV)
(C) Only (II), (IV), and (V)
(D) (I), (II), (III), (IV), and (V)

**May/June 2023**

**45.** Consider the following statements regarding the operation of NEFT:
I The originating bank branch sends the message to its NEFT Service Centre (pooling centre).
II The NEFT Clearing Centre is operated by the National Clearing Cell, Reserve Bank of India, Mumbai.
Which of the above statement(s) is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**Oct/Nov 2018**

**46.** The ability to initiate and receive timely confirmation of transfers between accounts at the central bank that become final within a brief period of time is defined as:
(A) Gridlock resolution finality
(B) Intraday finality
(C) Designated-time finality
(D) Deferred multilateral finality

Downloaded from www.pdf.tube

Q. First 4 characters
R. 5th character
S. Last 6 characters

List II: (Description/Format)

1. Represent the bank
2. 0 (zero)
3. 11 digits
4. Represent the branch

(A) P-1, Q-4, R-3, S-2
(B) P-4, Q-2, R-1, S-3
(C) P-3, Q-2, R-1, S-4
(D) P-3, Q-1, R-2, S-4

**May/June 2008**

**35.** Identify the correct statement regarding NG-RTGS.
(A) It was introduced by the RBI and upgraded to the industry standard ISO 20022 XML format.
(B) It was built by the central bank using strictly proprietary and closed-loop messaging protocols.
(C) It downgraded existing queue management features to prioritize traditional end-of-day net settlement.
(D) It removed the technical facility that allowed participants to accept future value dated transactions.

**Oct/Nov 2013**

**36.** Consider the following statements regarding the benefits of using NEFT:
I The remitter need not send the physical cheque or Demand Draft to the beneficiary.
II It is highly prone to the loss or theft of physical instruments during electronic transit.
III The remitter can track the transaction through the originating bank using a unique transaction reference number.
Which of the above statement(s) is/are correct?
(A) Only (I) and (II)
(B) Only (I) and (III)
(C) Only (II) and (III)
(D) (I), (II), and (III)

**May/June 2015**

**37.** Consider the following classifications of interbank funds transfer systems:
I Private sector systems where the central bank's main role is merely to act as the settlement agent.
II Central bank systems owned and operated by the central bank, which also provides settlement.
III Systems in which ownership and operation are fully restricted from being shared between the private sector and central bank.
Which of the above statement(s) is/are correct regarding systemic ownership models?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) (I), (II), and (III)

**Oct/Nov 2012**

**38.** A retail customer walks into a bank branch and wishes to transfer 1,50,000 to an account in another bank using RTGS. The teller refuses the transaction. What is the valid regulatory reason for this refusal?
(A) RTGS is strictly restricted to corporate entities and not available for retail customers.
(B) RTGS cannot process transactions during banking hours; it is strictly an after-hours batch process.
(C) The customer must possess a Positive Pay System authorization for any transaction above 50,000.
(D) The minimum amount to be remitted through RTGS is 2,00,000.

**May/June 2011**

**39.** Which of the following is not a valid restriction or limit associated with the NEFT system?
(A) Cash remittances by walk-in customers are strictly restricted to a maximum of 50,000 per transaction.
(B) The upper limit per transaction for the Indo-Nepal Remittance Facility is currently set at Rs. 2.00 lacs.
(C) Cash-based remittances to Nepal are capped at 50,000 per transaction to ensure regulatory compliance.
(D) Account-to-account remittances within India are capped at a maximum of 2,00,000 per transaction.

**Oct/Nov 2020**

**40.** The following question consists of two statements, an Assertion (A) and a Reason (R). Choose the correct option to describe the relationship between them.

NODIA

bank account. Under the Indo-Nepal Remittance Facility Scheme, what is the maximum amount the remitter can send if the transaction is cash-based?
(A) 50,000
(B) 1,00,000
(C) 2,00,000
(D) 5,00,000

**May/June 2005**

**55.** Identify the correct statement regarding the availability and limits of the RTGS system in India.
(A) The system is available 24x7x365 with effect from December 14, 2020.
(B) The maximum ceiling for an RTGS transaction is capped at 50,00,000.
(C) Banks are mandated to charge a flat RBI processing fee of 100 for every RTGS transaction.
(D) The RTGS system operates strictly in 48 half-hourly batches starting from 00:30 hours.

**Oct/Nov 2022**

**56.** Match the RTGS message flow structures in List I with their key operational features in List II.
List I: (Message Flow Structure)
P. V-shaped
Q. Y-shaped
R. L-shaped
S. T-shaped
List II: (Operational Feature)
1. Original message held at a system gateway; core subset sent for settlement.
2. Full message passed initially to the central bank.
3. Central processor strips core subset for settlement; full message rebuilt after settlement.
4. Sending bank transmits a copy of the full payment message to the central bank.
(A) P-2, Q-3, R-1, S-4
(B) P-1, Q-4, R-2, S-3
(C) P-3, Q-1, R-4, S-2
(D) P-2, Q-1, R-3, S-4

**May/June 2018**

**57.** The following question consists of two statements, an Assertion (A) and a Reason (R). Choose the correct option to describe the relationship between them.
Assertion (A): In case of a successful credit to the beneficiary's account via NEFT, the originating bank sends an acknowledgement to the originating customer.
Reason (R): The destination bank passes the credit to the beneficiary and sends an inward remittance message to the originating bank directly without involving the Clearing Centre.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2016**

**58.** Consider the following statements about Queuing Arrangements in RTGS:
I Queues can only be held at the system's central processor, never within the banks' internal systems.
II Queue management can be centralized or decentralized.
III Sending banks can hold funds transfer orders pending in a certain order to manage liquidity.
IV Centrally located queues and internal queues are mutually exclusive; banks cannot maintain both simultaneously.
Which of the above statement(s) is/are correct?
(A) Only (II) and (III)
(B) Only (I), (II), and (IV)
(C) Only (I) and (III)
(D) (I), (II), (III), and (IV)

**May/June 2014**

**59.** Identify the correct statement regarding the settlement mechanism in the National Electronic Fund Transfer (NEFT) system.
(A) NEFT settlement happens on a Real-Time and Gross Settlement basis continuously.
(B) NEFT is available only during regular banking hours and excluding public holidays.
(C) NEFT settlement happens in batches, with 48 half-hourly settlement batches daily.
(D) NEFT guarantees immediate 5-10 second credit confirmation directly to the receiver without clearing center involvement.

Click Here to Buy book on Amazon

Oct/Nov 2007

**60.** The Next Generation RTGS (NG RTGS) system is reportedly the first in the world to be built on which of the following messaging standards?
(A) SWIFT MT
(B) ISO 20022
(C) X.509
(D) IEEE 802.11

May/June 2025

**61.** Consider the following statements about the Aadhaar Enabled Payment System (AePS):
I It relies on a network of Micro ATMs using Aadhaar authentication.
II It is a bank-led model.
III It allows basic interoperable banking transactions through Business Correspondents.
IV It strictly limits transactions to large corporate fund transfers above 2,00,000.
Which of the above statement(s) is/are correct?
(A) Only (I), (II), and (III)
(B) Only (I), (III), and (IV)
(C) Only (II), (III), and (IV)
(D) (I), (II), (III), and (IV)

Oct/Nov 2019

**62.** Consider the following statements regarding services available under IMPS:
I It allows for sending and receiving money.
II It facilitates merchant payments, grocery bills, and travel & ticketing.
III Transactions can only be initiated from Bank branches; mobile and ATM channels are prohibited.
Which of the above statement(s) is/are correct?
(A) Only (I) and (II)
(B) Only (I) and (III)
(C) Only (II) and (III)
(D) (I), (II), and (III)

May/June 2009

**63.** Identify the incorrect statement regarding NPCI Bharat BillPay Limited (NBBL).
(A) It was conceptualized to handle Aadhaar Enabled Payment System (AePS) cash withdrawals.
(B) It was created as a new dedicated subsidiary for managing the Bharat Bill Payment System.
(C) It aims to increase growth especially in the business to consumer segment for small businesses.
(D) It is a public company registered in December 2020 to handle bill payment infrastructure.

Oct/Nov 2011

**64.** A customer is in a basement store with no telecom network or internet connection. They wish to make a payment of Rs 150 for groceries. According to RBI guidelines, can this transaction be executed digitally, and if so, how?
(A) No, all digital payments strictly require continuous internet connectivity.
(B) RTGS batch processing which does not require real-time internet.
(C) Yes, via an offline digital payment as the amount is within the Rs 200 per transaction limit.
(D) No, because offline payments are only allowed for amounts exceeding Rs 500.

May/June 2010

**65.** Identify the correct statement regarding the *99# USSD service.
(A) It uses quick codes for transactions and doesn't require a smartphone.
(B) It requires a high-speed broadband internet connection to function.
(C) It was developed by the SWIFT network to replace SFMS.
(D) It is an entirely private sector initiative without any integration into the Pradhan Mantri Jan Dhan Yojna.

Oct/Nov 2024

**66.** Under Bharat QR Code, which dynamic feature sets it apart from static QR code payments?
(A) The merchant generates a new code for every transaction, and the customer scanning it does not enter the amount.
(B) The customer manually enters the merchant's bank account number and IFSC into the app for every new transaction.
(C) The QR code system requires the physical swiping of a card to validate the transaction limit at the merchant site.
(D) The dynamic QR code infrastructure restricts payments to only Visa and MasterCard networks to maintain processing security.

NODIA

May/June 2017

**67.** The National Payments Corporation of India (NPCI) is a not-for-profit organisation registered under section 8 of the Companies Act 2013. In which year was NPCI founded?
(A) 2005
(B) 2008
(C) 2010
(D) 2013

Oct/Nov 2005

**68.** The following question consists of two statements, an Assertion (A) and a Reason (R). Choose the correct option to describe the relationship between them.
Assertion (A): Once a fund transfer is initiated via Aadhaar or UPI, money is debited from the payer's bank account and deposited in the recipient's bank account in real-time.
Reason (R): These payment systems are constrained by bank holidays and are only operational during regular clearing house hours.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2020

**69.** Identify the incorrect statement regarding the features of the Unified Payment Interface (UPI).
(A) A user must possess a credit card to set or change their UPI PIN in the BHIM App.
(B) Under UPI, users can make instant bank-to-bank payments using just a Mobile number or Virtual Payment Address (VPA).
(C) A user can collect money by entering a Virtual Payment Address and generating a collect request.
(D) Users can view their static QR code and share it through various messenger applications.

Oct/Nov 2015

**70.** Which of the following is not a supported payment mode under the Bharat Bill Payment System (BBPS)?
(A) Credit, Debit, and Prepaid Cards
(B) NEFT Internet Banking
(C) Foreign currency physical cash deposits
(D) Aadhaar based Payments and UPI

May/June 2013

**71.** Prior to the introduction of Bharat QR, what was the primary limitation of existing QR code-based payment gateways like mVisa or MasterPass?
(A) They were closed systems, where mVisa only worked for Visa and MasterPass for MasterCard holders.
(B) They required complex physical infrastructure like POS machines to scan the codes at retail counters.
(C) They were technically incapable of processing any transactions valued above a limit of 50,000.
(D) They were designed as legacy systems that were fundamentally incapable of operating on smartphones.

Oct/Nov 2021

**72.** Match the NPCI subsidiaries and services in List I with their primary functions in List II.
List I: (NPCI Entity/Product)
P. NIPL
Q. NBBL
R. RuPay
S. NFS
List II: (Primary Function)
1. Network of shared automated teller machines in India.
2. Domestic card scheme reducing international dependency.
3. Manages the Bharat Bill Payment System ecosystem.
4. Focuses on the internationalization of UPI and RuPay.
(A) P-1, Q-2, R-3, S-4
(B) P-4, Q-3, R-2, S-1
(C) P-4, Q-1, R-2, S-3
(D) P-3, Q-4, R-1, S-2

May/June 2024

**73.** Consider the following statements regarding Immediate Payment Service (IMPS):
I It is an instant real-time inter-bank electronic fund transfer service available 24x7 throughout the year including bank holidays.
II Upon initiation, the fund transfer via IMPS is completed within 5-10 seconds.
Which of the above statement(s) is/are correct?
(A) Only (I)

NODIA

(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**Oct/Nov 2008**

**74.** Identify the incorrect statement regarding recent digital payment helpline and feature phone initiatives.
(A) UPI Pay123 is a 3-step method to initiate and execute UPI services for feature phone users.
(B) DigiSaathi is a 24x7 helpline for digital payments launched by RBI.
(C) UPI Pay123 requires a mandatory 4G internet connection or an active USSD channel to operate.
(D) UPI Pay123 is based on Interactive Voice Response (IVR) technology, which is useful for rural areas.

**May/June 2006**

**75.** Consider the following statements regarding the proliferation of UPI:
I It was launched in 2016 and crossed 1 billion transactions for the first time in October 2019.
II The COVID-19 outbreak further accelerated its adoption.
III The volume and value of monthly UPI transactions nearly doubled from January to December 2021.
IV NPCI expects the UPI platform to eventually hit 100 crore transactions per day.
Which of the above statement(s) is/are correct?
(A) Only (I), (II), and (III)
(B) Only (II), (III), and (IV)
(C) Only (I), (III), and (IV)
(D) (I), (II), (III), and (IV)

**Oct/Nov 2017**

**76.** Identify the correct statement regarding NPCI International Payments Limited (NIPL).
(A) It was created exclusively to manage the National Financial Switch operations within India.
(B) It was dissolved after Malaysian company Merchantrade Asia launched its own internal network.
(C) It manages the Bharat Bill Payment System (BBPS) to increase growth in the B2C segment.
(D) Its primary focus is the internationalization of RuPay and the Unified Payment Interface (UPI).

**May/June 2008**

**77.** Which of the following is a limitation or negative exception recently updated regarding UPI transactions?
(A) It completely forbids linking multiple bank accounts to a single verified mobile number.
(B) It prohibits users from checking the balance of any linked bank accounts for security reasons.
(C) It does not support any QR code based payment initiations at merchant establishments.
(D) RBI limits offline UPI payments to Rs 200 per transaction and Rs 2,00,0 total.

**Oct/Nov 2013**

**78.** Consider the following statements regarding the Bharat Bill Payment System (BBPS):
I It is an RBI conceptualised system driven by the NPCI.
II It provides an interoperable "Anytime Anywhere" bill payment service.
III It allows payments exclusively through physical cash deposited at Bank Branches.
IV It offers an effective mechanism for handling consumer complaints.
V It supports multiple payment modes including UPI, Wallets, NEFT, and Cards.
Which of the above statement(s) is/are correct?
(A) Only (I), (II), (IV), and (V)
(B) Only (II), (III), (IV), and (V)
(C) Only (I), (III), and (IV)
(D) (I), (II), (III), (IV), and (V)

**May/June 2015**

**79.** The Mobile Money Identifier (MMID) is uniquely linked with an account number and helps in identifying the beneficiary in an IMPS transaction. The MMID consists of how many digits?
(A) 4 digits
(B) 7 digits
(C) 9 digits
(D) 11 digits

**Oct/Nov 2012**

**80.** Match the NPCI services in List I with their key descriptions in List II.
List I: (Service Name)

Downloaded from www.pdf.tube

P. BHIM
Q. Bharat QR
R. RuPay Contactless
S. IMPS

List II: (Description)

1. A real-time, 24x7 inter-bank electronic funds transfer system via mobile.
2. A mobile app acting as client software for UPI.
3. A contactless payment technology avoiding physical swipe.
4. A common code developed in collaboration with American Express, MasterCard, and Visa.

(A) P-1, Q-3, R-2, S-4
(B) P-4, Q-2, R-1, S-3
(C) P-2, Q-1, R-4, S-3
(D) P-2, Q-4, R-3, S-1

**May/June 2011**

**81.** Identify the incorrect statement regarding the Bharat QR Code system.
(A) It is the world's first interoperable payment platform based on a unified QR code.
(B) It integrates closed systems like Visa's mVisa, MasterCard's MasterPass, and RuPay into a common ground.
(C) It entirely rejects and blocks UPI-based payments such as BHIM.
(D) The QR codes are black and white two-dimensional machine readable codes storing merchant bank accounts and URLs.

**Oct/Nov 2020**

**82.** A migrant worker in Malaysia wants to send money back to his family in India instantaneously. He uses a service provided by Merchantrade Asia, which leverages Indian digital payment infrastructure. Which entity/product combination is primarily responsible for facilitating this international cross-border remittance via UPI infrastructure?
(A) NIPL and UPI
(B) SWIFT and SFMS
(C) NBBL and BBPS
(D) IDRBT and RTGS

**May/June 2022**

**83.** The Unified Payments Interface (UPI) integrates with more than 120 banks. Consumers can participate in P2P transfer as long as they both have an account in registered banks. What is the fundamental requirement generated by the user to authenticate these transfers on their mobile app?
(A) An IDRBT Crypto Card PIN
(B) A MAC Address Token
(C) A biometric iris recognition scan
(D) A BHIM UPI PIN

**Oct/Nov 2023**

**84.** A user repeatedly receives fraudulent requests to send money on their UPI application from an unknown VPA. Which feature of UPI is specifically designed to handle this issue?
(A) Scan & Pay
(B) Request Money
(C) Block/Spam User
(D) Check Balance

**May/June 2016**

**85.** A farmer in a remote village possesses a basic feature phone with no internet capability and wants to check his bank balance and transfer funds. He dials a quick code and navigates a menu provided by his telecom operator. Which specific service is the farmer utilizing?
(A) RTGS Web-API
(B) Bharat QR
(C) *99# USSD
(D) BHIM Aadhaar Pay

NODIA

**Oct/Nov 2009**

**86.** Which of the following best represents the achievement of NPCI regarding the RuPay card network?
(A) It mandated that all cooperative banks issue only Visa or MasterCard for cards.
(B) It launched a domestic card network, successfully reducing dependency on international schemes.
(C) It completely eliminated the use of the National Financial Switch for all digital payments.
(D) It restricted card issuance solely to the Pradhan Mantri Jan Dhan Yojana account holders.

**May/June 2023**

**87.** The following question consists of two statements, an Assertion (A) and a Reason (R). Choose the correct option to describe the relationship between them.
Assertion (A): IMPS has gained popularity

(B) The Central Hub System
(C) Off-line Servers (Thick Clients)
(D) A generic Web Browser

**May/June 2014**

**101.** A branch handles accounts for a state government department. To relay Government Account Transactions securely over the intra-bank SFMS network to the central reporting office, which message format is designated for this purpose?
(A) IFN 298 G Series
(B) IFN 298 C Series
(C) IFN 598 S Series
(D) n98

**Oct/Nov 2007**

**102.** Identify the correct statement regarding the Bank Gateway in the SFMS architecture.
(A) It switches Intra-Bank messages between Branch Servers and forwards Inter-Bank messages to the Hub.
(B) It connects directly to the Internet for processing without interfacing with the centralized Hub System.
(C) It stores all copies of user-generated messages locally on On-line terminals for archival at each branch.
(D) It acts primarily as a thick client interface for message creation at remote branches within the bank.

**May/June 2025**

**103.** Consider the following Intra-Bank message types in SFMS:
I IFN 100, 102 - Customer TTs
II IFN 110, 111 & 112 - DD related messages
III IFN 202, 203 - Transfer of Funds to another Bank
IV IFN 760, 769 - Messages relating to Bank Guarantees
Which of the above correctly map the message type to the transaction?
(A) Only (I), (II), and (IV)
(B) Only (II), (III), and (IV)
(C) Only (I), (III), and (IV)
(D) (I), (II), (III), and (IV)

**Oct/Nov 2019**

**104.** Identify the incorrect statement regarding the types of clients/terminals in SFMS.
(A) On-line terminals (Thin Clients) are PCs that use a standard browser to connect to the Branch Server.
(B) Copies of messages are permanently stored on On-line terminals to allow offline viewing.
(C) Off-line Servers (Thick Clients) are PCs provided with the SFMS Off-line software module.
(D) Off-line Servers allow off-line creation, verification, authorization, viewing, and processing of messages.

**May/June 2009**

**105.** The following question consists of two statements, an Assertion (A) and a Reason (R). Choose the correct option to describe the relationship between them.
Assertion (A): SFMS is an Electronic Data Interchange (EDI) system that allows the exchange of structured messages prepared in conformity with published standards.
Reason (R): SFMS relies on a Working Group on Message Standards to publish the standard message formats for use within the network.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2011**

**106.** The following question consists of two statements, an Assertion (A) and a Reason (R). Choose the correct option to describe the relationship between them.
Assertion (A): Going cashless via Bharat QR Code drastically brings down the total costs involved for both the consumer and the merchant.
Reason (R): Bharat QR Code eliminates the requirement of PoS machines for swiping cards, involves no transaction cost, and reduces the time consumed to make the payment.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).

Click Here to Buy book on Amazon

text message transmission.
Which of the above statement(s) is/are correct?
(A) Only (I), (II), (III), and (IV)
(B) Only (II), (III), (IV), and (V)
(C) Only (I), (II), and (III)
(D) (I), (II), (III), and (IV)

**Oct/Nov 2006**

**94.** Match the IFN series in List I with their corresponding financial message categories in List II.
List I: (IFN Series)
P. IFN 202, 203
Q. IFN 400, 410, 412
R. IFN 700, 701, 705
S. IFN 900 & 910
List II: (Message Category)
1. Debit/Credit Advices
2. Transfer of Funds to another Bank
3. Documentary Credit related messages
4. Messages relating to Collection Bills
(A) P-1, Q-2, R-4, S-3
(B) P-4, Q-3, R-1, S-2
(C) P-2, Q-4, R-3, S-1
(D) P-3, Q-4, R-1, S-2

**May/June 2021**

**95.** In SFMS Security, how is the confidentiality of a message protected while it is in transit?
(A) By encrypting it with the sender node's Private Key.
(B) By encrypting it with the receiving node's Public Key.
(C) By sending it as plain text over a closed VPN.
(D) By hashing the message without any encryption.

**Oct/Nov 2010**

**96.** Arrange the logical sequence of user roles involved in securely dispatching a financial message through the SFMS system:
I. The Verifier checks and digitally signs the outgoing message.
II. The Authorizer gives final approval by appending their digital signature to the message.
III. The Creator drafts the message and saves it to the system.
IV. The message travels securely over the network to the destination node.
(A) I, III, II, IV
(B) III, I, II, IV
(C) III, II, I, IV
(D) II, I, III, IV

**May/June 2005**

**97.** A small retail merchant wants to start accepting digital payments from customers using Visa, MasterCard, RuPay, and UPI apps without investing in a physical Point-of-Sale (PoS) swiping machine and avoiding transaction costs. Which system best fulfills this requirement?
(A) RTGS
(B) CTS-2010
(C) MICR Sorter
(D) Bharat QR Code

**Oct/Nov 2022**

**98.** Match the requirement of Public Key Certificates (PKC) in SFMS to their respective entities.
List I: (PKC Requirement)
P. User PKCs
Q. Server Signing PKCs
R. Server Encryption PKCs
S. Secure Server PKCs
List II: (Applicable Entity)
1. For Every SFMS Server (viz., Hub, CGBS, Gateway) to encrypt data.
2. For any Server where the Bank feels it is necessary to restrict access to HTTPS mode.
3. For Every User at Gateway or CGBS, Verifier, Authorizer, or Super User.
4. For Every SFMS Server to digitally sign data.
(A) P-3, Q-4, R-1, S-2
(B) P-1, Q-2, R-3, S-4
(C) P-4, Q-3, R-2, S-1
(D) P-3, Q-1, R-4, S-2

**May/June 2018**

**99.** Identify the correct pair linking the proprietary/free format message type to its designated alphanumeric code in SFMS.
(A) n98 — Free Format Letters to RBI
(B) n98 — Proprietary Returns & Statements
(C) n99 — Proprietary Returns & Statements
(D) IFN 985 — G-Sec Transactions

**Oct/Nov 2016**

**100.** A rural bank branch faces intermittent network connectivity issues. To ensure continuous message creation, verification, and authorization without depending on an active link to the Branch Server, the branch should install:
(A) On-line Terminals (Thin Clients)

NODIA

as it allows a sender to transfer funds to a beneficiary's account instantly on a Sunday.
Reason (R): Unlike NEFT, which settles in batches during specified hours, IMPS is available 24x7 round the clock, including on bank holidays.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2018**

**88.** FASTag is a device used for making toll payments directly from an associated account while the vehicle is in motion. What core technology does FASTag employ?
(A) Magnetic Ink Character Recognition (MICR)
(B) Radio Frequency Identification (RFID)
(C) Near Field Communication (NFC) via RuPay Contactless
(D) Electronic Data Interchange (EDI)

**May/June 2007**

**89.** Identify the correct combination of options available for a customer to perform an IMPS transaction.
(A) Beneficiary Email ID and UPI PIN; Virtual Payment Address and destination IFSC Code.
(B) Beneficiary Mobile no. and MMID; Account no. and IFS Code; Aadhaar Number.
(C) Beneficiary Cheque Number and MICR code; Beneficiary Mobile no. and current IFSC Code.
(D) Beneficiary Debit Card number and CVV; Beneficiary Account no. and specific MMID code.

**Oct/Nov 2025**

**90.** Which centralized clearing service aims at providing interbank high volume, low value transactions that are repetitive and periodic in nature?
(A) National Automated Clearing House (NACH)
(B) National Electronic Fund Transfer (NEFT)
(C) Real Time Gross Settlement (RTGS)
(D) Structured Financial Messaging System (SFMS)

**May/June 2012**

**91.** What is the primary advantage for a bank opting for the Common Gateway cum Branch Server (CGBS) software module in SFMS?
(A) It strictly segregates the Gateway and Branch Server hardware to maximize redundancy across the network.
(B) It allows installing Gateway and Branch modules on one Server, saving on license and admin costs.
(C) It eliminates the need for X.509 digital signatures for all internal transactions within the bank.
(D) It forces all domestic transactions to be routed through the international SWIFT network for verification.

**Oct/Nov 2014**

**92.** The following question consists of two statements, an Assertion (A) and a Reason (R). Choose the correct option to describe the relationship between them.
Assertion (A): User Banks can generate SWIFT messages at remote Branches using SFMS and relay the same to the SWIFT Gateway (CBT) for onward transmission.
Reason (R): SFMS messages strictly conform to SWIFT standards, making this interface technically possible and cost-effective.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2019**

**93.** Consider the following statements about the Structured Financial Messaging System (SFMS):
I It is an Indian standard similar to SWIFT.
II It is nicknamed the indigenous SWIFT of India.
III The inter-bank messaging part is used by applications like NEFT and RTGS.
IV It provides APIs to integrate existing and future applications.
V It exclusively supports unencrypted, plain

Downloaded from www.pdf.tube

(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2010**

**107.** A branch manager wishes to send a secure, intra-bank message regarding a Demand Draft issue to another branch of the same bank. Which specific SFMS message format should the creator select for this transaction?
(A) IFN 110
(B) IFN 100
(C) IFN 298 C
(D) IFN 760

**Oct/Nov 2024**

**108.** Match the SFMS architectural components in List I with their functions in List II.
List I: (SFMS Component)
P. Hub System
Q. Bank Gateway
R. Branch Server
S. Thin Client
List II: (Function)
1. Uses a standard browser to connect without requiring SFMS software modules.
2. Located at IDRBT, switches messages between different banks.
3. Switches Intra-Bank messages and connects to the Hub.
4. Allows users to create, verify, and authorize outgoing messages.
(A) P-2, Q-3, R-4, S-1
(B) P-3, Q-2, R-1, S-4
(C) P-2, Q-4, R-3, S-1
(D) P-4, Q-1, R-2, S-3

**May/June 2017**

**109.** In the context of SFMS, what fundamental operational difference distinguishes Inter-Bank messages that require settlement from those that do not?
(A) Settlement messages require the exchange of encrypted magnetic tapes, whereas non-settlement messages use online networks.
(B) Settlement messages must be in Free Format (n99), whereas non-settlement messages strictly use IFN 100.
(C) Settlement messages can bypass the SFMS Hub, whereas non-settlement messages must route through it.
(D) Settlement messages necessarily involve the receipt/payment of funds between contra-party banks, often relying on RBI's RTGS system.

NODIA

**Oct/Nov 2005**

**110.** A branch initiates a critical fund transfer. The Creator inputs the details, the Verifier confirms it, and the Authorizer gives the final approval. Upon reaching the destination bank, a dispute arises weeks later about the message's authenticity. How does the SFMS system technically resolve this dispute?
(A) By retrieving the printed paper copy of the transaction from the files at the originating branch.
(B) By cross-referencing the MAC address of the Thin Client used by the creator at the time of entry.
(C) By checking the authorizing official's digital signature stored and archived with the message.
(D) By relying on the SWIFT network's centralized dispute resolution APIs for all inter-bank messages.

**May/June 2020**

**111.** A corporate client requests their bank to execute an urgent Telegraphic Transfer (TT) to another account within the same bank. The operating officer processing the transaction via SFMS will use which message type?
(A) IFN 760
(B) IFN 420
(C) IFN 900
(D) IFN 100

**Oct/Nov 2015**

**112.** Identify the incorrect statement regarding SFMS authentication and archival.
(A) When a message is verified, the verifier has to digitally sign the message for security purposes.
(B) The authorizer's signature is appended to the message and travels to the destination SFMS Server.
(C) Signatures are stored with the archived message to prevent any altering of messages after archival.
(D) After processing at the destination, the signature is stripped and only the plain text is archived.

May/June 2013

**113.** Consider the following statements regarding SFMS user roles:

I Creator users are only allowed to create, list, and view messages.

II Authorizer users create and maintain other user accounts.

Which of the above statement(s) is/are correct?

(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

Oct/Nov 2021

**114.** Identify the incorrect statement regarding SFMS message types and their corresponding transactions.

(A) IFN 210 — Funds expected from another Bank
(B) IFN 298 G Series — Currency Chest reports to RBI
(C) IFN 400 series — Messages relating to Collection Bills
(D) IFN 700 series — Documentary Credit related messages

May/June 2024

**115.** Consider the following statements regarding SFMS Message Usage:

I SFMS messages cover every conceivable method of information interchange between any two offices of a bank.

II SFMS can only be used for relaying messages that have a direct financial implication.

III Every message is relayed in strict confidence and authenticated with the digital signature of the authorizing official.

Which of the above statement(s) is/are correct?

(A) Only (I) and (II)
(B) Only (I) and (III)
(C) Only (II) and (III)
(D) (I), (II), and (III)

Oct/Nov 2008

**116.** Within the SFMS Architecture, which entity is located at IDRBT, Hyderabad and is responsible for switching Inter-Bank messages from the sending Bank's Gateway to the receiving Bank's Gateway?

(A) Branch Server
(B) Common Gateway cum Branch Server
(C) Off-line Server
(D) Hub System

May/June 2006

**117.** Consider the following statements regarding the creation of SWIFT messages on SFMS Terminals:

I It requires Swift Interface Modules.

II It brings considerable savings in investment for SWIFT message preparation software at remote branches.

III It ensures properly legally enforceable authentication of messages between remote branches and the SWIFT Gateway.

IV It leads to a reduction in SWIFT training costs for operatives at remote branches.

V It requires each remote branch to establish a direct leased line to the SWIFT international hub bypassing the bank's CBT.

Which of the above statement(s) is/are correct?

(A) Only (I), (II), (III), and (IV)
(B) Only (II), (III), (IV), and (V)
(C) Only (I), (III), (IV), and (V)
(D) (I), (II), (III), (IV), and (V)

Oct/Nov 2017

**118.** The following question consists of two statements, an Assertion (A) and a Reason (R). Choose the correct option to describe the relationship between them.

Assertion (A): Access control for Verifier, Authorizer, and Super Users in SFMS requires them to sign the login message with their private keys stored in smart cards.

Reason (R): SFMS demands high-level security, utilizing X.509 Digital signatures and PKCs to authenticate users accessing any SFMS Server.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2008

**119.** Which of the following Inter-Bank messages sent over SFMS is an exception, meaning it does NOT require immediate or prior settlement of funds?

(A) Letters and Circulars sent to RBI (n99 Free Format)

Click Here to Buy book on Amazon

(B) Customer TTs (IFN 100)
(C) Transfer of Funds to another Bank (IFN 202)
(D) DD related messages (IFN 110)

**Oct/Nov 2013**

**120.** Which of the following user categories in SFMS relies solely on passwords for Access Control rather than digitally signing the login message with a private key?
(A) Creator users
(B) Verifier users
(C) Authorizer users
(D) Super users

**May/June 2015**

**121.** The Lead Bank of a district needs to circulate a machine-readable statistical return to the RBI. Since this involves no fund settlement but requires strict formatting, which SFMS message type should the Lead Bank use?
(A) n99
(B) IFN 985
(C) IFN 298 G
(D) n98 (Proprietary)

**Oct/Nov 2012**

**122.** A bank agrees to issue a Bank Guarantee on behalf of a construction firm. The issuing branch must notify the beneficiary's branch. Which inter-bank message type (which does not require prior settlement) is used over SFMS to transmit this guarantee?
(A) IFN 210
(B) IFN 430
(C) IFN 760
(D) IFN 910

**May/June 2011**

**123.** Consider the following consolidated statements regarding clearing limits and payment systems:
I The Positive Pay System involves re-confirmation of cheque details for amounts beyond 50,000.
II The minimum amount to be remitted through RTGS is 2,00,000 with no upper ceiling.
III Walk-in cash remittances under NEFT are restricted to a maximum of 50,000 per transaction.
IV Offline digital payments on UPI are allowed up to Rs 200 per transaction.
V The upper limit per transaction for the Indo-Nepal Remittance Facility is Rs 2.00 lacs.
Which of the above statement(s) accurately reflect the numerical limits of these systems?
(A) Only (I), (II), (III), and (IV)
(B) Only (II), (III), (IV), and (V)
(C) Only (I), (III), (IV), and (V)
(D) (I), (II), (III), (IV), and (V)

**Oct/Nov 2020**

**124.** Match the specific Inter-Bank message types that do not require prior settlement in List I with their corresponding IFN formats in List II.
List I: (Inter-Bank Message)
P. Currency Chest reports to RBI
Q. G-Sec related messages
R. Opinion Reports and requests for Opinion
S. Messages relating to Collection Bills
List II: (IFN Format)
1. IFN 985 & 986
2. IFN 400, 410, 412
3. IFN 598 S Series
4. IFN 298 C Series
(A) P-4, Q-3, R-1, S-2
(B) P-3, Q-4, R-2, S-1
(C) P-4, Q-1, R-3, S-2
(D) P-1, Q-2, R-3, S-4

**May/June 2022**

**125.** A primary dealer bank executes a trade involving Government Securities. To relay the message regarding the G-Sec transaction without involving immediate funds settlement across the SFMS network, which message type is appropriate?
(A) IFN 102
(B) IFN 598 S Series
(C) IFN 202
(D) IFN 700

www.nodia.in

Downloaded from www.pdf.tube

bank name, the fifth character is always zero, and the last six characters identify the branch. IFSC codes help ensure secure, accurate, and fast transfer of funds between banks through digital banking and electronic payment systems.

**50.** (C) USSD *99# dial-in interface
The ISO 20022 compliant RTGS system provides several advanced access options for financial institutions, including Thick-client interfaces, Web-API connectivity via the INFINET, and a specialized Payment Originator module. These tools allow banks to manage high-value transactions efficiently based on their volume and infrastructure. However, the USSD interface is a separate retail service designed for basic mobile banking and is not a core RTGS access method.

**51.** (A) II, IV, I, III
An NEFT transaction follows a precise chronological sequence starting with the originating branch preparing the message and sending it to its pooling center. The pooling center then forwards this data to the central NEFT Clearing Centre. Next, the Clearing Centre sorts these transactions by destination bank and prepares the accounting entries. Finally, the destination bank receives the messages and credits the beneficiary's account.

**52.** (D) Because it could be implemented by modifying rather than rewriting the existing DNS software arrangement.
The L-shaped message flow structure was preferred for systems like CHAPS because it offered a cost-effective path for modernization. Instead of completely rewriting the complex software used for previous deferred net settlement arrangements, banks could modify the existing logic. This architecture allows internal gateways to manage full messages while only sending settlement-related subsets to the central bank, facilitating a smoother transition to gross settlement.

**53.** (C) Simultaneous final transfers of both securities and funds on a trade-by-trade basis.
A real-time Delivery Versus Payment system is designed to eliminate principal risk by ensuring that the transfer of securities occurs only if the corresponding transfer of funds is finalized. This requires both the securities and funds legs to be settled simultaneously on a transaction-by-transaction basis. By linking the RTGS system with a Securities Settlement System, the architecture ensures that neither party is exposed during the trade.

**54.** (A) 50,000
The Indo-Nepal Remittance Facility Scheme allows for the transfer of funds to Nepal, even for those without bank accounts. For such cash-based transactions, a regulatory limit of fifty thousand rupees per remittance is applied to ensure compliance with financial safety standards. This service provides a critical link for migrant workers to send money home to relatives who may lack access to formal banking infrastructure.

**55.** (A) The system is available 24x7x365 with effect from December 14, 2020.
Since December 2020, India's RTGS system has operated on a round-the-clock basis every day of the year, providing continuous settlement for high-value transactions. While there is a minimum threshold of two lakhs for initiating a transfer, there is no maximum ceiling imposed by the regulator. Furthermore, the Reserve Bank of India has waived its processing fees to encourage wider adoption of electronic payments.

**56.** (A) P-2, Q-3, R-1, S-4
RTGS architectures are classified by how messages move between banks and the central hub. In V-shaped structures, the full message passes to the central bank first. Y-shaped structures involve a central processor that strips data for settlement and rebuilds the message afterward. L-shaped structures hold the full message at a gateway while sending subsets for settlement, and T-shaped structures involve sending copies to the central bank.

**57.** (C) Assertion (A) is true, but Reason (R) is false.
In a successful NEFT transaction, the originating bank sends an acknowledgement to the customer once the credit is confirmed. However, the destination bank does not communicate directly with the originating bank. Instead, all transaction messages and status updates are routed through the central NEFT Clearing Centre, which acts as the hub for sorting, settlement, and relaying

only legitimate, authorized cheques are cleared, protecting against forgery and alterations.

**9.** (B) P-1, Q-2, R-3, S-4
Debit clearing systems are specifically designed for collecting periodic payments, such as utility bills for electricity and gas, while reducing printing and courier costs for service providers. Conversely, credit clearing systems facilitate the distribution of periodical dividend or interest payments to multiple beneficiaries. These systems help companies avoid the manual reconciliation tasks associated with numerous outstanding warrants and printed documents.

**10.** (C) P-2, Q-4, R-1, S-3
The lower white band of a cheque contains specifically formatted encoded fields for automated processing. The cheque number is a six-digit code, followed by a nine-character field for the center code. The transaction code is represented by a two-character field identifying account types, while the amount is encoded using a thirteen-digit field. These precise formats enable magnetic ink character recognition readers.

**11.** (C) Assertion (A) is true, but Reason (R) is false.
Netting involves the accumulation of multiple transactions to offset credits against debits, resulting in a single net obligation. By its very nature, this accumulation requires a delay to group transactions, making it fundamentally incompatible with continuous, real-time settlement. In contrast, real-time gross settlement systems process each transaction individually and immediately, ensuring that finality is achieved without waiting for a netting cycle.

**12.** (C) All MICR cheques presented during the day are strictly processed manually during regular banking hours to ensure immediate credit.
Magnetic Ink Character Recognition technology utilizes specialized encoders and high-speed reader-sorters to automate cheque processing at clearing houses. These machines identify characters printed in magnetic ink to facilitate rapid sorting and data extraction. Contrary to manual processing methods, this automated system is designed to handle large volumes of instruments efficiently, with final payment and returns typically managed through organized clearing cycles.

**13.** (A) The Positive Pay System
Starting from January 2021, banks implemented a mandatory confirmation rule for high-value cheques to enhance transaction security. Under this system, the issuer must provide specific details of the cheque to the drawee bank electronically. If the issuer fails to utilize this re-confirmation process, the bank may return the cheque unpaid, even if the account holds sufficient funds to cover the amount.

**14.** (C) Stopping the physical cheque flow to the drawee and replacing it with electronic images and data.
Cheque truncation is the process where the physical movement of a cheque is stopped at some point in the clearing cycle. Instead of transporting the paper instrument to the drawee branch, an electronic image and relevant data are transmitted for processing. This modern approach reduces transit time, lowers costs, and minimizes the risks associated with the physical handling of negotiable instruments.

**15.** (D) Settlement of funds occurs on a transaction-by-transaction basis without netting.
Gross settlement systems are characterized by the individual processing of every funds transfer instruction. Each transaction is settled independently and immediately, rather than being grouped or offset against other transfers. This architecture ensures that funds move from the sending bank to the receiving bank on a transaction-by-transaction basis, providing immediate finality and eliminating the risks inherent in deferred net settlement models.

**16.** (A) 9 digits
The center code, also known as the MICR code, is a nine-digit numerical sequence printed on the lower band of a cheque. This code is crucial for automated sorting and clearing as it identifies the specific city, bank, and branch associated with the instrument. The first three digits represent the city, followed by three for the bank, and three for the branch.

Click Here to Buy book on Amazon

**33.** (B) The full message is passed to the central bank and sent to the receiver after settlement.
The V-shaped message flow structure is defined by the central bank acting as the primary hub for both communication and settlement. A sending bank transmits the entire payment instruction to the central bank. Once the settlement is successfully finalized in the central bank's accounts, the central bank then transmits the full original message to the receiving bank, completing the electronic fund transfer.

**34.** (D) P-3, Q-1, R-2, S-4
The Indian Financial System Code is an eleven-character alphanumeric code used for electronic funds transfers. Its structure is precisely defined: the first four characters identify the bank name, followed by the fifth character which is always a zero. The final six characters represent the specific branch of that bank. This standardized format ensures that every branch in the country is uniquely identifiable.

**35.** (A) It was introduced by the RBI and upgraded to the industry standard ISO 20022 XML format.
Next Generation RTGS represents a significant upgrade to India's large-value payment infrastructure, adopting the globally recognized ISO 20022 messaging standard. This XML-based format allows for richer data transmission and improved interoperability between financial systems. The system also introduced advanced features like improved queue management, multi-currency capabilities, and the ability for participants to accept future value-dated transactions, enhancing overall liquidity management.

**36.** (B) Only (I) and (III)
National Electronic Fund Transfer provides numerous advantages, such as eliminating the need to send physical cheques or demand drafts to beneficiaries. This electronic method significantly reduces the risk of loss or theft associated with paper instruments. Furthermore, remitters can easily track their transactions using unique reference numbers provided by the bank, ensuring transparency and providing timely confirmations for successful fund transfers.

NODIA

**37.** (A) Only (I) and (II)
Interbank funds transfer systems are typically classified by their ownership and operational models. Some systems are owned and operated entirely by the central bank, which also provides the final settlement. Alternatively, private sector systems may exist where the central bank's primary role is limited to acting as the settlement agent. These models facilitate a range of payment architectures suited to different market needs.

**38.** (D) The minimum amount to be remitted through RTGS is 2,00,000.
The RTGS system is specifically designed for high-value transactions, and regulatory guidelines set a minimum floor for its use. Currently, the minimum amount that can be remitted through this system is two lakhs. If a customer attempts to send a smaller amount, such as one lakh fifty thousand, the bank will refer them to the NEFT system instead, which has no minimum limit.

**39.** (D) Account-to-account remittances within India are capped at a maximum of 2,00,000 per transaction.
National Electronic Fund Transfer is a versatile system with specific limits for certain types of transactions. Cash remittances by walk-in customers are capped at fifty thousand rupees, and the Indo-Nepal Remittance Facility has its own defined caps. However, for standard account-to-account transfers within India, there is no regulatory upper limit imposed by the system, allowing users to move large sums of money.

**40.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
In RTGS environments, transactions are settled immediately if the sending bank has sufficient liquidity in its central bank account. When funds are inadequate, the system places these instructions into a queue. This queuing arrangement is a vital liquidity management tool that prevents banks from breaching limits or overdrafting, ensuring that payments are settled in an orderly fashion as soon as funds become available.

**25.** (B) Increased collection charges for cheques drawn on a bank within the grid.
The Cheque Truncation System offers numerous benefits, including faster clearing cycles, reduced operational risks, and enhanced reconciliation. It is designed to increase efficiency for both banks and customers by eliminating the need to physically move cheques. Contrary to increasing costs, the system aims to reduce transit-related expenses; therefore, an increase in collection charges for grid-based transactions is not a stated benefit.

**26.** (D) First three digits represent the city, next three represent the bank, last three represent the branch.
The nine-digit MICR center code printed on a cheque is structured logically to facilitate automated sorting. The first three digits identify the specific city where the branch is located. The middle three digits indicate the bank to which the cheque belongs. Finally, the last three digits specify the individual branch of that bank, allowing the clearing system to route the instrument accurately.

**27.** (A) Designated-time settlement systems
Designated-time settlement systems are classified by their practice of final fund settlement occurring at specific, pre-defined intervals during the business day. Unlike real-time systems that settle transactions immediately as they occur, these systems accumulate instructions over a period. They may use netting mechanisms to calculate final obligations, which are then settled at the appointed times, providing a predictable schedule for financial institutions.

**28.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Cheque truncation effectively eliminates the physical movement of paper instruments between bank branches during the clearing process. This is achieved by truncating the cheque at the collecting bank and transmitting a high-quality electronic image along with the relevant MICR data to the drawee bank. Because the electronic record serves as the basis for payment, the physical instrument is only moved in rare, exceptional circumstances.

**29.** (C) A listed company disbursing annual dividends to 50,000 investors.
A credit clearing system is most appropriate for scenarios involving the disbursement of funds from a single source to a large number of beneficiaries. In the case of a listed company paying dividends to fifty thousand investors, this system automates the process by pushing credits directly into the recipients' bank accounts. This method is far more efficient than printing and mailing thousands of physical warrants.

**30.** (D) They are image friendly and possess enhanced security features.
CTS-2010 standards were introduced to ensure that all cheques used in India are suitable for electronic imaging and automated processing. These compliant cheques feature standardized security elements, such as specific watermarks and paper quality, which help prevent fraud and alterations. By being "image-friendly," they ensure that the electronic representations captured during truncation are clear, legible, and legally valid for clearing and settlement purposes.

**31.** (C) V-shaped structure — Network operator independently handles all message routing without the central bank.
In a V-shaped RTGS structure, the sending bank transmits the full payment message to the central bank. The central bank processes the settlement and subsequently forwards the complete message to the receiving bank. It is incorrect to state that a network operator handles routing independently without the central bank in this specific architecture, as the central bank remains the core routing hub.

**32.** (B) RTGS
Real Time Gross Settlement is the appropriate system for large-value, time-critical transfers because it settles transactions individually and immediately. Unlike NEFT, which operates in batches and may experience delays, RTGS ensures that funds move from the remitter to the beneficiary instantaneously. Since the transaction amount of twenty-five lakhs exceeds the minimum RTGS threshold, it provides the fastest and most secure settlement method available.

Downloaded from www.pdf.tube

# ANSWERS

1. (D) The cheque can contain minor folds and minimal tabs on either end to assist automated sorting.
Standardized physical specifications for cheques ensure high-speed processing through magnetic ink character recognition readers. While precise white bands and specialized magnetic ink are required for accurate encoding and scanning, physical defects like folds or tabs are prohibited. Such imperfections interfere with the mechanical sorting process, potentially causing jams or errors in automated clearing systems.

2. (A) Only (I), (II), and (III)
Debit clearing systems facilitate repetitive payments by allowing service providers to pull funds directly from customer accounts based on prior authorization. This mechanism is ideal for utility bills, as it reduces manual tracking of due dates and printing tasks. The service provider manages the mandate and submits it to the bank, which then processes the necessary debits.

3. (C) It eliminates manual encoding by capturing cheque images directly.
Optical Character Recognition technology represents an advancement over Magnetic Ink Character Recognition by enabling the direct capture of cheque images. This process removes the need for manual encoding of data into magnetic bands, which is a requirement for MICR-based systems. By digitizing the physical document, OCR streamlines the workflow and enhances the speed of modern electronic clearing.

4. (C) Real Time Gross Settlement System
Real Time Gross Settlement systems process funds transfer instructions on a continuous, transaction-by-transaction basis. Unlike net settlement systems that accumulate transactions and resolve balances periodically, RTGS ensures that each transfer is settled individually and immediately in central bank money. This architecture provides finality and significantly reduces systemic risks associated with interbank payment obligations and delayed settlements.

5. (B) Only (I) and (III)
Cheque truncation significantly improves clearing efficiency by replacing the physical movement of cheques with electronic images. This modernization enables faster realization of proceeds, often within the same day, and eliminates geographical barriers to clearing. Furthermore, centralized image archival and secure transmission routes reduce operational risks, ensuring that transactions are handled with high security and improved verification and reconciliation capabilities.

6. (B) Large-value DNS systems are incompatible with the transmission and processing of payment messages in real time.
Designated-time Net Settlement systems calculate the net position of participating banks by subtracting total funds sent from total funds received. These systems can operate on a bilateral or multilateral basis, with final settlement occurring at specific intervals. Notably, DNS systems are technically compatible with real-time message transmission, even if the final settlement of funds is deferred to a later time.

7. (B) Clearing House
A clearing house serves as a centralized intermediary where banks meet to settle interbank cheques drawn on one another. This common service, available in both metropolitan and smaller cities, simplifies the exchange process by consolidating multiple claims. By facilitating the netting of mutual obligations, the clearing house ensures efficient fund movement and reduces the physical handling required for individual bank settlements.

8. (B) To enhance the safety of cheque-based transactions and prevent fraud.
The Positive Pay System is a fraud prevention mechanism that requires the issuer of a high-value cheque to re-confirm essential details with their bank. By verifying information such as the date, beneficiary name, and amount before processing, the system adds a critical layer of security. This procedure ensures that

NODIA

**41.** (B) NEFT — Facilitates one-to-one funds transfer occurring in batches.
The National Electronic Fund Transfer system is a deferred net settlement mechanism where transactions are processed in half-hourly batches rather than individually. It facilitates one-to-one funds transfers across the country, but final settlement only occurs at the end of each batch interval. This batch processing architecture distinguishes NEFT from real-time systems like RTGS, which settle each transaction individually and immediately upon receipt.

**42.** (C) The full business information exchanged between sending and receiving banks is fully known to the settlement agent.
In a Y-shaped message flow structure, a central processor acts as an intermediary. The sending bank transmits the full message to this processor, which then extracts only a core subset of data required for settlement to send to the central bank. Consequently, the settlement agent does not have access to the full business information, preserving a level of privacy for the participants.

**43.** (B) If banks choose to levy charges for RTGS transactions, RBI has set the cap at Rs 500 for each transaction.
The Reserve Bank of India manages RTGS and has taken steps to lower costs for users, including waiving processing charges for banks. While banks are permitted to levy service charges on customers for initiating RTGS transactions, these fees are strictly regulated and capped at much lower levels than five hundred rupees. The specific caps depend on the transaction value and the channel used.

**44.** (A) Only (I), (III), (IV), and (V)
The Next Generation RTGS system introduced advanced technical features such as gridlock resolution mechanisms and various access modules like Web-API and Payment Originator. It provides participants with flexible participation modes and supports future value-dated transactions. Contrary to limited capabilities, NG-RTGS was designed with modern standards to handle multi-currency transactions and provide a robust infrastructure for the country's high-value payment and settlement requirements.

**45.** (C) Both (I) and (II)
The NEFT transaction flow begins at the originating branch, which transmits the payment message to its internal pooling center or service center. These centers then forward the consolidated messages to the central NEFT Clearing Centre. This central hub is operated by the National Clearing Cell of the Reserve Bank of India in Mumbai, where transactions are sorted by destination bank for settlement and credit.

**46.** (B) Intraday finality
Intraday finality refers to the capability within a payment system to achieve the final settlement of funds transfer instructions during the processing day. This means that once a transfer is confirmed between bank accounts at the central bank, it becomes irrevocable and unconditional within a very short timeframe. This feature is a hallmark of real-time systems, providing certainty to participants and reducing risk.

**47.** (B) To open an account or use an existing account, as cash-based NEFT transfers are capped at 50,000.
Regulatory guidelines for NEFT limit cash-based transactions for walk-in customers without an account to a maximum of fifty thousand rupees. If a customer needs to transfer sixty-five thousand rupees, they must either use an existing bank account or open a new one to facilitate the full amount. This ensures compliance with anti-money laundering regulations and maintains the integrity of the electronic payment system.

**48.** (B) L-shaped structure
An L-shaped message flow structure is often chosen when upgrading existing systems because it allows for modifications rather than a complete rewrite. In this architecture, the sending bank's gateway holds the full payment message while transmitting only a subset of information to the central bank for settlement. The full message is only released to the receiving bank once a settlement confirmation is received.

**49.** (B) 11 digits
The Indian Financial System Code (IFSC) is an 11-character alpha-numeric code used to identify specific bank branches in India for electronic payment systems such as NEFT, RTGS, and IMPS. The first four characters represent the

Click Here to Buy book on Amazon

**17.** (A) Only (I)
Credit clearing systems offer significant advantages to corporate entities by automating the distribution of funds to numerous beneficiaries simultaneously. This system eliminates the need to print and mail a large volume of dividend or interest warrants, thereby reducing administrative costs and operational efforts. Beneficiaries receive credits directly into their bank accounts, removing the requirement for them to visit a branch physically.

**18.** (A) Only (I)
On a cheque's lower band, the transaction code is a two-character field that designates the specific type of account, such as savings or current. This code helps automated systems categorize the transaction for proper processing. Other fields include the six-digit cheque number and the nine-digit center code. Together, these encoded elements facilitate accurate and rapid identification within the banking clearing infrastructure.

**19.** (D) Debit clearing pulls funds from customers' accounts periodically for utilities, whereas credit clearing distributes funds like dividends to multiple beneficiaries.
The fundamental distinction between debit and credit clearing lies in the direction of fund movement and the initiation process. Debit clearing is a "pull" mechanism used by organizations to collect recurring payments from various customers based on prior mandates. In contrast, credit clearing is a "push" mechanism used to disburse funds, such as dividends or interest, from one source to many recipients.

**20.** (A) Customers must physically visit the branch to re-confirm cheque details without exception.
The Positive Pay System allows customers to re-confirm key details of high-value cheques issued by them through multiple convenient digital channels. While it is mandatory for certain transaction values, users typically provide this information via mobile banking, internet banking, or SMS rather than being forced to visit a physical branch. Failure to confirm these details may lead to the cheque being returned during clearing.

**21.** (C) Real Time Gross Settlement (RTGS) System
Real Time Gross Settlement systems are designed to settle large-value funds transfers on a transaction-by-transaction basis. By operating continuously, these systems provide immediate finality and eliminate the credit and systemic risks found in netting-based architectures. Settlement occurs in central bank money, ensuring the highest level of safety and reliability for interbank transactions, which is essential for maintaining financial market stability.

**22.** (B) To move electronic images instead of physical instruments, reducing payment time and transit costs.
The primary goal of the Cheque Truncation System is to modernize the clearing process by replacing physical instrument movement with electronic image transmission. This shift significantly reduces the time required for payment realization and lowers the operational costs associated with transporting paper cheques. By utilizing high-resolution images and MICR data, CTS enhances security, improves reconciliation, and streamlines clearing across broad geographical regions.

**23.** (D) Positive Pay System
The Positive Pay System mandates that the issuer of a high-value cheque, typically above fifty thousand rupees, must provide specific confirmation details to the bank. These details include the date, payee name, and exact amount. If a cheque for five lakhs fifty thousand is presented without this prior notification, the bank is authorized to return it unpaid to prevent potential fraudulent activity.

NODIA

**24.** (D) Debit Clearing System
A debit clearing system allows service providers to collect bill payments directly from customer bank accounts using pre-approved mandates. This model is highly efficient for utility companies, as it automates the collection process and eliminates the need for manual bill dispatch and payment tracking. By pulling the required funds on due dates, the system ensures timely payments and reduces administrative overhead.

information between the participating financial institutions.

**58.** (A) Only (II) and (III)
Queuing is an essential liquidity management feature in RTGS systems, allowing banks to hold transfer orders until sufficient funds are available in their central bank accounts. These queues can be managed in either a centralized manner at the system hub or a decentralized manner within the banks' own internal systems. Banks often maintain both types of queues simultaneously to prioritize and sequence their outgoing payments.

**59.** (C) NEFT settlement happens in batches, with 48 half-hourly settlement batches daily.
The National Electronic Fund Transfer system operates on a deferred net settlement basis rather than real-time. It processes transactions in forty-eight half-hourly batches every day, providing a continuous but batched cycle of fund movements. This schedule allows the system to settle numerous small-value transactions efficiently throughout the day and night, ensuring that credits reach beneficiaries within a predictable timeframe following each batch's completion.

**60.** (B) ISO 20022
The Next Generation RTGS system was a pioneer in adopting the ISO 20022 messaging standard for high-value payments. This internationally recognized XML-based format provides a common language for financial data, allowing for more detailed information and improved interoperability across global networks. By moving away from older, less flexible protocols, NG-RTGS offers enhanced security, better tracking, and a robust platform for future financial innovations and complex transactions.

**61.** (A) Only (I), (II), and (III)
The Aadhaar Enabled Payment System is a bank-led model designed to facilitate basic interoperable banking transactions through business correspondents. It utilizes a network of micro-ATMs where customers can perform tasks like withdrawals and balance inquiries using Aadhaar authentication. This system is specifically aimed at promoting financial inclusion in rural areas and is not restricted to high-value corporate transfers, making banking accessible to the unbanked.

**62.** (A) Only (I) and (II)
Immediate Payment Service is a versatile real-time funds transfer mechanism that supports both person-to-person and person-to-merchant transactions. Users can conveniently send and receive money for various purposes, including paying for groceries, travel, and utility bills. Unlike traditional systems that might be restricted to branch operations, IMPS is designed for accessibility across multiple digital channels, including mobile apps, internet banking, and ATMs, ensuring round-the-clock availability.

**63.** (A) It was conceptualized to handle Aadhaar Enabled Payment System (AePS) cash withdrawals.
NPCI Bharat BillPay Limited is a dedicated subsidiary established to manage and grow the Bharat Bill Payment System ecosystem. Its primary focus is on providing a unified and interoperable bill payment platform for consumers and small businesses, particularly in the business-to-consumer segment. It is not responsible for the Aadhaar Enabled Payment System, which is a separate infrastructure managed directly under the National Payments Corporation of India.

**64.** (C) Yes, via an offline digital payment as the amount is within the Rs 200 per transaction limit.
RBI guidelines permit offline digital payments to facilitate transactions in areas with poor or no internet connectivity. These payments are currently allowed for small-value transactions, with a limit of two hundred rupees per individual transaction. Since the grocery bill is one hundred and fifty rupees, it can be executed using authorized offline payment methods, which later synchronize with the banking system when a connection is restored.

**65.** (A) It uses quick codes for transactions and doesn't require a smartphone.
The *99# service utilizes Unstructured Supplementary Service Data technology to provide basic banking services via mobile phones. This system is particularly beneficial because it does not require a smartphone or an active data connection, making it accessible to users with feature phones. By dialing the specific quick code, users can perform transactions, check balances,

NODIA

and access financial services integrated with the national payment infrastructure.

**66.** (A) The merchant generates a new code for every transaction, and the customer scanning it does not enter the amount.
A dynamic Bharat QR code enhances the payment experience by embedding the specific transaction amount directly into the generated image. When a merchant creates this code for a purchase, the customer simply scans it with their mobile app, and the payment is authorized without the need for manual amount entry. This reduces errors and streamlines the checkout process compared to static QR codes where users must input totals.

**67.** (B) 2008
The National Payments Corporation of India was established in 2008 as an initiative of the Reserve Bank of India and the Indian Banks' Association. Registered as a not-for-profit company, its primary mandate is to create a robust and modern payment and settlement infrastructure for the entire country. Since its inception, NPCI has launched several transformative products, including RuPay, IMPS, and the Unified Payments Interface.

**68.** (C) Assertion (A) is true, but Reason (R) is false.
Payment systems like UPI and Aadhaar-enabled services facilitate the real-time debit and credit of funds between accounts instantaneously. These modern digital infrastructures are designed for continuous operation and are not constrained by traditional bank holidays or clearing house hours. They provide round-the-clock availability, ensuring that users can move money and complete transactions at any time of the day or night, regardless of banking schedules.

**69.** (A) A user must possess a credit card to set or change their UPI PIN in the BHIM App.
To set or change a UPI PIN within the BHIM application, a user typically requires a valid debit card associated with their bank account rather than a credit card. The system uses debit card details for authentication to ensure that the person initiating the PIN setup is the authorized account holder. Once established, this PIN is used to authorize all future transactions and fund transfers securely.

**70.** (C) Foreign currency physical cash deposits
The Bharat Bill Payment System is designed to be highly interoperable, supporting a wide range of domestic payment modes including credit and debit cards, internet banking, UPI, and Aadhaar-based payments. While it facilitates bill payments through various digital and physical channels, it does not support transactions using physical foreign currency. The system is focused on domestic currency settlements within the Indian financial ecosystem for utility and service bills.

**71.** (A) They were closed systems, where mVisa only worked for Visa and MasterPass for MasterCard holders.
Before the introduction of Bharat QR, existing QR code solutions were largely proprietary and operated as closed-loop systems. For instance, mVisa was limited to Visa cardholders, while MasterPass was reserved for those with MasterCard. This lack of interoperability meant that merchants had to display multiple QR codes for different networks, creating confusion and inefficiency. Bharat QR solved this by providing a unified, interoperable standard.

**72.** (B) P-4, Q-3, R-2, S-1
The NPCI ecosystem consists of various entities and products with specialized roles. NIPL focuses on expanding UPI and RuPay to international markets, while NBBL manages the interoperable Bharat Bill Payment System. RuPay serves as the domestic card network to reduce reliance on global schemes. Finally, the National Financial Switch operates the extensive network of shared automated teller machines across the country to ensure interoperability.

**73.** (C) Both (I) and (II)
Immediate Payment Service is a robust electronic fund transfer platform that provides instant, real-time settlement for inter-bank transactions. It is uniquely characterized by its round-the-clock availability, functioning 24x7 throughout the year, including weekends and public holidays. Once a user initiates a transfer, the system is designed to complete the entire process and credit the beneficiary's account within a brief period of five to ten seconds.

Downloaded from www.pdf.tube

74. (C) UPI Pay123 requires a mandatory 4G internet connection or an active USSD channel to operate.
UPI Pay123 is specifically designed to bring digital payment capabilities to feature phone users without requiring a 4G internet connection. It leverages Interactive Voice Response technology, allowing users to initiate and complete transactions through a simple three-step process over a standard phone call. This innovation ensures that digital financial services are accessible in rural areas where high-speed internet and smartphones may be less prevalent.

75. (D) (I), (II), (III), and (IV)
Since its launch in 2016, the Unified Payments Interface has seen exponential growth, particularly following the COVID-19 pandemic which accelerated digital adoption. It surpassed one billion monthly transactions in late 2019 and continued to nearly double in volume throughout 2021. With its widespread acceptance, the platform is expected to reach massive daily transaction milestones, reflecting its status as a cornerstone of India's retail payment infrastructure.

76. (D) Its primary focus is the internationalization of RuPay and the Unified Payment Interface (UPI).
NPCI International Payments Limited is a wholly-owned subsidiary established to take India's successful digital payment innovations to the global stage. Its main objective is to facilitate the internationalization of RuPay cards and the UPI platform. By partnering with international financial institutions and payment providers, NIPL enables cross-border remittances and allows Indian travelers to use their familiar payment methods in foreign countries.

77. (D) RBI limits offline UPI payments to Rs 200 per transaction and Rs 2,000 total.
While UPI offers great flexibility, certain regulatory limits are placed on specific transaction types to manage risk. For offline payments intended for use in areas with poor connectivity, the Reserve Bank of India has set a maximum limit of two hundred rupees for any single transaction. Additionally, there is a cumulative limit of two thousand rupees for such offline transactions before a synchronization with the network is required.

78. (A) Only (I), (II), (IV), and (V)
The Bharat Bill Payment System is an interoperable ecosystem designed by the RBI and managed by NPCI to provide a convenient "anytime anywhere" bill payment service. It supports numerous digital payment modes, including UPI, wallets, and internet banking, and offers a robust mechanism for consumer complaint redressal. While it aims for widespread accessibility, it is primarily a digital-first platform rather than one restricted to physical branch cash deposits.

79. (B) 7 digits
The Mobile Money Identifier is a unique seven-digit code issued by banks to customers who register for mobile banking. When combined with a mobile number, the MMID acts as a specific identifier for a bank account, enabling the routing of funds through the Immediate Payment Service. This system allows users to receive money instantly without sharing sensitive details like their full bank account number or IFSC code.

NODIA

80. (D) P-2, Q-4, R-3, S-1
NPCI provides a suite of digital payment products with distinct functionalities. BHIM is a mobile application that serves as client software for UPI transactions. Bharat QR is an interoperable code standard developed with major international card networks. RuPay Contactless utilizes technology that allows payments without a physical swipe. IMPS is the underlying 24x7 inter-bank funds transfer system that facilitates real-time mobile and electronic payments across India.

81. (C) It entirely rejects and blocks UPI-based payments such as BHIM.
Bharat QR is designed to be the world's first fully interoperable payment platform, integrating various card networks like RuPay, Visa, and MasterCard into a single code. Contrary to blocking other systems, it is built to be inclusive and fully supports UPI-based payments, including those initiated through the BHIM application. This interoperability allows merchants to accept payments from a wide range of customer apps using a single, unified QR code.

82. (A) NIPL and UPI
To facilitate international cross-border remittances leveraging India's digital

infrastructure, NPCI International Payments Limited works with global partners. By integrating the Unified Payments Interface with international networks like Merchantrade Asia in Malaysia, NIPL enables migrant workers to send money home instantaneously. This partnership allows funds to be credited directly to Indian bank accounts using the efficiency and security of the UPI platform on a global scale.

**83.** (D) A BHIM UPI PIN
To ensure the security and authorization of funds transfers initiated through a mobile app, the Unified Payments Interface requires users to enter a specific UPI PIN. This personal identification number is set by the user and must be entered for every transaction to confirm the sender's identity and intent. It serves as the final authentication layer, protecting the user's bank account from unauthorized access and fraudulent transfers.

**84.** (C) Block/Spam User
The UPI platform includes a specialized feature that allows users to block or report specific Virtual Payment Addresses that send suspicious or fraudulent money requests. By using the "Block/Spam" option, a user can stop receiving notifications and requests from unknown or malicious actors. This protective measure is essential for maintaining a secure user experience and preventing individuals from accidentally authorizing fraudulent "collect" requests from scammers.

**85.** (C) *99# USSD
For users in remote areas without internet or smartphones, the *99# USSD service provides a critical link to digital banking. By dialing this code on a basic mobile phone, a user can access a text-based menu provided by their telecom operator. This interface allows them to perform essential tasks such as checking bank balances and transferring funds, leveraging the national payment infrastructure through simple, non-data-dependent communication protocols.

**86.** (B) It launched a domestic card network, successfully reducing dependency on international schemes.
One of the most significant achievements of NPCI was the development and launch of RuPay, India's own domestic card payment network. By creating this local infrastructure, NPCI successfully reduced the country's reliance on international card schemes like Visa and MasterCard. This initiative has lowered transaction costs for banks and merchants, improved data sovereignty, and expanded financial inclusion by making cards more accessible to a broader population.

**87.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
The Immediate Payment Service has become highly popular because it offers the convenience of instant funds transfers at any time, including Sundays and public holidays. This is possible because IMPS is designed as a 24x7 real-time system, unlike some traditional clearing methods that operate only during specific hours or in batches. This round-the-clock availability ensures that beneficiaries receive funds within seconds of the transaction being initiated by the sender.

**88.** (B) Radio Frequency Identification (RFID)
FASTag utilizes Radio Frequency Identification technology to enable automatic toll collection at highway plazas. A small RFID-enabled tag is fixed to the vehicle's windshield, which is read by sensors as the car passes through the toll lane. The system then automatically deducts the required fee from the linked prepaid or bank account, allowing for seamless travel without the need for the vehicle to stop for cash payments.

**89.** (B) Beneficiary Mobile no. and MMID; Account no. and IFS Code; Aadhaar Number.
IMPS provides multiple flexible ways for users to initiate an instant fund transfer. A sender can use the beneficiary's mobile number along with their seven-digit Mobile Money Identifier to route the payment. Alternatively, the transaction can be completed using the traditional combination of a bank account number and the corresponding IFSC code. In some cases, the beneficiary's Aadhaar number can also serve as the identifier.

**90.** (A) National Automated Clearing House (NACH)
The National Automated Clearing House is a centralized service designed to handle high-volume, low-value transactions that are periodic and repetitive. It is widely used by institutions for distributing salaries, dividends, and pensions, as well as for collecting recurring payments

Click Here to Buy book on Amazon

like utility bills and loan installments. By consolidating these transactions into a unified electronic platform, NACH improves efficiency and reduces the administrative burden on banks and corporate entities.

**91.** (B) It allows installing Gateway and Branch modules on one Server, saving on license and admin costs.
The Common Gateway cum Branch Server module in the Structured Financial Messaging System provides a cost-effective solution for banks by consolidating multiple functions onto a single hardware platform. By allowing the Gateway and Branch Server modules to coexist on one server, banks can significantly reduce their software licensing fees and administrative overhead. This integrated approach simplifies system management while maintaining the high security and reliability required for financial messaging.

**92.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Banks can generate SWIFT-compatible messages at remote branches using the Structured Financial Messaging System and relay them through their central SWIFT gateway. This is technically feasible because SFMS was designed to conform strictly to international SWIFT standards. This integration allows financial institutions to leverage their existing domestic infrastructure to process international transactions, resulting in significant cost savings and improved operational efficiency for cross-border financial communication and funds transfer.

**93.** (A) Only (I), (II), (III), and (IV)
The Structured Financial Messaging System is India's domestic equivalent to the international SWIFT network, providing a secure and standardized platform for inter-bank communication. It serves as the backbone for critical applications like NEFT and RTGS, using encrypted messages and digital signatures to ensure integrity and confidentiality. SFMS also offers flexible APIs for integration with various banking software, ensuring it can adapt to evolving financial technologies and transaction requirements.

NODIA

**94.** (C) P-2, Q-4, R-3, S-1
In the Structured Financial Messaging System, different IFN series codes are designated for specific financial activities. The 200 series, such as IFN 202, is used for transferring funds between banks. The 400 series manages messages related to collection bills, while the 700 series is reserved for documentary credit. Finally, the 900 series, including IFN 900 and 910, is used for providing debit and credit advices to participants.

**95.** (B) By encrypting it with the receiving node's Public Key.
To ensure that a financial message remains confidential while traveling across the SFMS network, the system employs public-key cryptography. The sender node encrypts the message content using the unique public key of the intended receiving node. This ensures that only the recipient, who possesses the corresponding private key, can decrypt and read the message, thereby preventing unauthorized access or interception by any third party during transmission.

**96.** (B) III, I, II, IV
The secure dispatch of a financial message in SFMS follows a logical multi-step workflow involving different authorized users. First, a Creator drafts the message details and saves them. Next, a Verifier reviews the content and appends their digital signature. An Authorizer then provides the final approval by adding a second digital signature. Once fully authorized, the message is transmitted securely over the network to reach its designated destination node.

**97.** (D) Bharat QR Code
For a retail merchant wanting to accept various digital payments without the expense of a physical Point-of-Sale machine, Bharat QR Code is the ideal solution. It allows customers to pay using UPI, RuPay, Visa, or MasterCard simply by scanning a printed code with their smartphones. This system eliminates the need for hardware maintenance and card swiping, providing a low-cost, efficient, and interoperable way for small businesses to go cashless.

**98.** (A) P-3, Q-4, R-1, S-2
Security in the Structured Financial Messaging System is maintained through various Public

# CHAPTER 11
# Plastic Money

Oct/Nov 2016

**1.** What is the length of the numeric code used for the CVV or CSC number on an American Express branded credit or debit card?
(A) 3 digits
(B) 4 digits
(C) 5 digits
(D) 6 digits

May/June 2009

**2.** The Secure Electronic Transaction (SET) protocol maintains a high level of confidentiality during online transactions. How does SET achieve this conceptual objective?
(A) By storing the customer's PIN directly on the merchant's local web server for future authorization.
(B) By bypassing the payment gateway and linking the buyer directly to the seller's specific bank branch.
(C) By blocking credit card details from the merchant so only the involved bank can access the data.
(D) By utilizing symmetric encryption to ensure the merchant can authorize the transaction locally.

Oct/Nov 2023

**3.** What does the term 'Interchange' refer to in the credit card business?
(A) The interest charged to a cardholder for carrying balances into a new cycle.
(B) The process of resolving transactions authorized by the acquirer but disputed.
(C) The commission earned by the acquirer and shared with the issuing bank.
(D) The recurring fee paid by a merchant to lease a point-of-sale terminal.

May/June 2018

**4.** Identify the correct statement outlining the usage of CVV numbers.
(A) The CVV number serves the exact same functional purpose as the cardholder's secret Personal Identification Number (PIN).
(B) A cardholder must always enter their PIN when an online merchant requests the CVV number.
(C) Providing the CVV to an online merchant proves the user possesses the physical card and helps reduce fraud.
(D) CVV numbers offer absolute protection against Phishing scams and fraudulent websites.

Oct/Nov 2011

**5.** The basic difference between a credit card and a debit card centers on the source of funds. Which of the following conceptually distinguishes the two?
(A) Credit cards are linked directly to personal deposit accounts, while debit cards rely on a line of credit.
(B) Debit cards require a deposit balance, while credit cards utilize a bank-sanctioned credit limit.
(C) Debit card transactions are billed monthly, while credit card payments are deducted from accounts instantly.
(D) Credit cards are for high-value transactions, while debit cards are restricted to small-value purchases.

May/June 2014

**6.** Identify the correct statement concerning the Secure Socket Layer (SSL) protocol.
(A) SSL is the latest standard that has completely replaced the Transport Layer Security protocol.
(B) Websites use SSL to authenticate identity, verified by the https prefix and a padlock symbol.
(C) SSL operates by directly encrypting the merchant's physical terminal to prevent card cloning.
(D) Transactions on websites lacking SSL certification are highly recommended for faster processing.

Downloaded from www.pdf.tube

This standardization ensures that messages can be automatically processed by different computer systems without human intervention, which is the core principle of EDI.

**106.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Adopting the Bharat QR Code system significantly lowers transaction costs for both merchants and consumers in the digital payment ecosystem. By using a simple, machine-readable code, merchants avoid the substantial investment and maintenance fees associated with physical Point-of-Sale swiping machines. Furthermore, the system streamlines the payment process, reducing the time spent at checkout and eliminating many of the fees typically associated with traditional card-based transactions at retail outlets.

**107.** (A) IFN 110
In the Structured Financial Messaging System, specific IFN formats are reserved for different types of internal banking communications. When one branch needs to inform another about the issuance of a Demand Draft, it uses the IFN 110 message type. This structured format ensures that the receiving branch gets all the necessary details to honor the draft when it is presented for payment, maintaining the integrity and security of the bank's internal operations.

**108.** (A) P-2, Q-3, R-4, S-1
The SFMS architecture consists of various components that work together to ensure secure message delivery. The Hub System at IDRBT handles the switching of inter-bank messages, while the Bank Gateway manages intra-bank traffic and connects to the Hub. Branch Servers provide the interface for users to create and authorize messages locally. Finally, Thin Clients offer a browser-based access method for users without requiring specialized software on their individual machines.

**109.** (D) Settlement messages necessarily involve the receipt/payment of funds between contra-party banks, often relying on RBI's RTGS system.
The primary distinction between inter-bank messages in SFMS lies in whether they trigger a movement of funds between the involved financial institutions. Settlement messages are used for actual fund transfers and typically rely on the Reserve Bank of India's RTGS system to finalize the payment obligations. In contrast, non-settlement messages are purely informational, such as opinion reports or guarantee notifications, and do not involve immediate financial reconciliation between the sending and receiving banks.

**110.** (C) By checking the authorizing official's digital signature stored and archived with the message.
The Structured Financial Messaging System ensures the legal enforceability and authenticity of every message through the use of digital signatures. When an Authorizer approves a message, their unique digital signature is appended and travels with the data. This signature is also preserved when the message is archived. In the event of a dispute, this archived signature provides incontrovertible proof of who authorized the transaction, preventing any future denial of the message's content.

**111.** (D) IFN 100
When a corporate client requests an urgent Telegraphic Transfer within the same bank, the operating officer uses the IFN 100 message type in the SFMS system. This specific format is designed for customer funds transfers and ensures that the details are transmitted securely and accurately between branches. By utilizing the standardized IFN 100 series, the bank can process these high-priority transfers efficiently while maintaining full audit trails and security through digital authentication.

**112.** (D) After processing at the destination, the signature is stripped and only the plain text is archived.
To maintain a high level of security and non-repudiation, the digital signatures of the verifier and authorizer are critical components of an SFMS message. These signatures are appended to the message during transmission and are intentionally preserved in the archive after the transaction is processed at the destination. Stripping the signature would undermine the system's ability to verify the message's integrity or prove its authenticity in the event of a future dispute.

NODIA

(A) They require rigorous real-time authentication with the issuer's central database for every purchase.
(B) They are processed based on data stored across the physical tracks of a magnetic stripe card.
(C) They carry monetary value and transactions do not necessitate the use of a formal bank account.
(D) They offer unlimited lines of credit determined by the spending habits of the individual user.

**May/June 2022**

**15.** In the sequence of an e-commerce transaction, which statement is correct?
(A) The payment gateway deposits funds directly into the buyer's account at a scheduled time.
(B) The seller's bank verifies the buyer's card details and approves or denies the transaction without contacting the issuer.
(C) E-commerce services mandate three-factor authentication for all domestic transactions in India.
(D) The payment gateway forwards the transaction information from the e-commerce checkout to the seller's bank.

**Oct/Nov 2008**

**16.** How is a 'Floor Limit' defined in the context of credit card transactions?
(A) A per-transaction limit where merchants may accept cards without prior authorization.
(B) The maximum total credit limit granted to a cardholder for monthly expenditures.
(C) The maximum commission rate an acquiring bank can deduct from merchant drafts.
(D) The minimum transaction amount required for a merchant to process card payments.

**May/June 2012**

**17.** Regarding the technical capabilities of smart cards versus magnetic stripe cards, which statement is correct?
(A) Smart cards store more data than magnetic stripe cards and can perform calculations on that data.
(B) Magnetic stripe cards possess a significantly higher data storage capacity than modern smart cards.
(C) Both smart cards and magnetic stripe cards store all their information on an embedded computer chip.
(D) Smart cards rely entirely on online validation, whereas magnetic stripe cards can validate offline.

**Oct/Nov 2015**

**18.** According to data released by the Reserve Bank of India, what was the market share of the RuPay card network in India's card market in the year 2020?
(A) 15%
(B) 30%
(C) 60%
(D) 90%

**May/June 2019**

**19.** Tokenization replaces sensitive card data with an alternate code. What is the conceptual role of a 'token vault' in this process?
(A) It is a hardware security module installed physically at the merchant's retail checkout location.
(B) It is an offline repository maintained by the cardholder to manually generate and track tokens.
(C) It is a specialized terminal designed to read EMV chips and tokens simultaneously at the point of sale.
(D) It is a database storing the link between the sensitive card value and its corresponding token.

**Oct/Nov 2017**

**20.** Contactless smart cards communicate seamlessly with a reader. How does the embedded chip in a contactless smart card conceptually draw operational power?
(A) It is powered on when brought into the electromagnetic field of the reader.
(B) It contains a miniature integrated battery with a limited lifespan.
(C) It receives power through physical contact pins located on the surface of the card.
(D) It utilizes kinetic energy generated by the swiping motion at the terminal.

**May/June 2011**

**21.** Which statement correctly identifies the characteristics of Near Field Communication (NFC)?

Click Here to Buy book on Amazon

levels of responsibility, such as verifiers and authorizers, are required to use more secure methods like digital signatures for login and transaction approval to ensure non-repudiation.

**121.** (D) n98 (Proprietary)
For the transmission of machine-readable statistical data that does not involve fund settlement, the Structured Financial Messaging System provides the "n98" proprietary message format. This code allows institutions like Lead Banks to send formatted returns to the Reserve Bank of India in a structured manner. Using n98 ensures that while the data is non-standard compared to typical financial transfers, it is still transmitted through a secure, authenticated channel that supports automated data extraction.

**122.** (C) IFN 760
A bank branch issuing a guarantee on behalf of a client must notify the beneficiary's branch using a specific inter-bank message type that does not require prior fund settlement. In SFMS, the IFN 760 format is designated for messages relating to bank guarantees. This standardized electronic communication ensures that the receiving branch is officially and securely informed of the guarantee's terms and authenticity, allowing for reliable coordination without the need for immediate inter-bank reconciliation.

**123.** (D) (I), (II), (III), (IV), and (V)
Various electronic payment systems in India are governed by specific numerical limits to manage risk and ensure efficiency. High-value cheques require re-confirmation via Positive Pay for amounts exceeding fifty thousand rupees. RTGS is reserved for transfers above two lakhs, while NEFT limits cash-based walk-in transactions to fifty thousand per instance. Additionally, offline UPI payments are capped at two hundred rupees, and the Indo-Nepal facility has been updated with a limit of two lakh rupees.

**124.** (A) P-4, Q-3, R-1, S-2
The SFMS system uses specific IFN codes for various non-settlement inter-bank messages. Reports for currency chests are sent using the IFN 298 C series, while government securities messages utilize the IFN 985 and 986 formats. For opinion reports, the IFN 598 S series is employed. Finally, messages related to collection bills are categorized under the IFN 400 series. These codes allow for precise identification and processing of different types of informational and administrative financial communications.

**125.** (B) IFN 598 S Series
In the context of government securities trading, banks use the Structured Financial Messaging System to relay messages that do not always involve immediate funds settlement. The IFN 598 S series is specifically appropriate for these types of G-Sec related communications across the network. This specialized message format ensures that the details of the security transaction are communicated securely between primary dealers and other participants, maintaining the integrity of the securities market's underlying messaging infrastructure.

www.nodia.in

Downloaded from www.pdf.tube

**113.** (A) Only (I)
Within the Structured Financial Messaging System, user roles are strictly defined to ensure a secure separation of duties. Creator users are responsible for drafting, listing, and viewing messages, but they do not have the authority to verify or approve them. The task of creating and maintaining user accounts is typically reserved for a Super User rather than an Authorizer, who is primarily responsible for the final approval and digital signing of outgoing financial messages.

**114.** (B) IFN 298 G Series — Currency Chest reports to RBI
The Structured Financial Messaging System uses various IFN series to categorize transactions correctly. While the 700 series handles documentary credit and the 400 series manages collection bills, the IFN 298 G series is specifically designated for government account transactions rather than currency chest reports. Identifying the correct message format is essential for ensuring that financial data is routed and processed according to the appropriate regulatory and operational requirements of the banking system.

**115.** (B) Only (I) and (III)
SFMS is a comprehensive platform designed to facilitate virtually every type of structured information exchange between bank offices. While it is the backbone for financial transfers, its utility extends beyond direct financial implications to include administrative and informational messages. Every communication on the network is held in strict confidence and authenticated using the digital signature of an authorizing official, ensuring the highest standards of data integrity and non-repudiation for all participants.

**116.** (D) Hub System
The Hub System is a central component of the SFMS architecture, physically located at the Institute for Development and Research in Banking Technology in Hyderabad. Its primary function is to act as a central switch for all inter-bank messages. When a bank gateway sends a message intended for another financial institution, the Hub receives it and routes it to the receiving bank's gateway, ensuring secure and standardized communication across the entire domestic banking network.

**117.** (A) Only (I), (II), (III), and (IV)
Integrating SWIFT message creation into SFMS terminals allows remote bank branches to prepare international messages using existing infrastructure. This approach requires specific interface modules but results in significant savings on specialized software and training for personnel. It also provides a legally enforceable method for authenticating messages before they reach the central SWIFT gateway. Crucially, this setup leverages the bank's internal network rather than requiring individual leased lines for every remote branch.

**118.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
High-level security in SFMS is achieved through robust access control mechanisms for sensitive user roles like verifiers and authorizers. These individuals must use private keys, often stored on secure smart cards, to digitally sign their login messages. This process relies on X.509 Digital Signatures and Public Key Certificates to uniquely authenticate every user. By requiring this cryptographic proof, the system ensures that only authorized personnel can access and process financial messages on the SFMS servers.

NODIA

**119.** (A) Letters and Circulars sent to RBI (n99 Free Format)
While most inter-bank messages in the Structured Financial Messaging System involve the movement of funds and require settlement through the RTGS system, certain categories are purely informational. For example, free-format letters and circulars sent to the Reserve Bank of India using the n99 format do not involve financial reconciliation. These messages utilize the secure SFMS infrastructure for authenticated communication and administrative purposes rather than for actual fund transfers or the exchange of negotiable instruments.

**120.** (A) Creator users
Within the multi-layered security framework of the Structured Financial Messaging System, different user roles have varying levels of access control. Creator users, who are responsible for inputting the initial details of a message, typically rely on standard password-based authentication to enter the system. In contrast, roles with higher

**Oct/Nov 2014**

**7.** Which of the following provides the most accurate definition of a bank credit card?
(A) A card used to withdraw physical cash from designated bank terminals.
(B) A revolving consumer loan that automatically renews within specific limits.
(C) A prepaid card that requires monetary loading before a purchase occurs.
(D) A tool that initiates an immediate deduction from a personal deposit account.

**Oct/Nov 2025**

**8.** Security codes play different roles depending on the transaction type. What conceptually distinguishes CVC1 from CVC2?
(A) CVC1 is for card-not-present transactions, while CVC2 is used specifically for all contactless payments.
(B) CVC1 is for card-present magnetic stripe verification, while CVC2 is for card-not-present transactions.
(C) CVC1 is a dynamic code that refreshes hourly, whereas CVC2 remains static on the reverse of the card.
(D) CVC1 validates identity via biometrics, while CVC2 encrypts data during the payment gateway transmission.

**May/June 2007**

**9.** Which of the following statements correctly describes the process of 'Charge Backs'?
(A) It refers to the interest charged by the issuer when a cardholder carries over the balance each month.
(B) It is a disputed transaction where the bank claims back the payment amount from the acquirer.
(C) It represents the commission earned by the acquiring bank for processing merchant sales drafts.
(D) It is the amount refunded to the customer by the merchant for returning defective or unwanted goods.

**Oct/Nov 2005**

**10.** In which year was the e-commerce technology called Motioncode (Dynamic CVV) introduced?
(A) 1996
(B) 2015
(C) 2016
(D) 2022

**May/June 2021**

**11.** Identify the correct statement regarding the scope of Card Tokenization in India.
(A) Tokenization has been mandated for both domestic and international e-commerce transactions.
(B) Consumers who choose not to have their card details stored do not require to follow tokenisation for one-time purchases.
(C) Banks will charge a nominal fee to customers for the issuance and management of tokens.
(D) Tokens generated are universal and a single token can be utilized across multiple distinct merchants.

**Oct/Nov 2010**

**12.** What is the fundamental definition of Card Tokenization?
(A) The implementation of dynamic verification codes that refresh automatically every hour to prevent skimming.
(B) The integration of smartcard functions with biometrics to authenticate the identity of the cardholder.
(C) The replacement of actual card details with a unique alternate code to securely process online transactions.
(D) The mandatory upgrade of all retail cash registers to read embedded microprocessor circuits instead of magnetic stripes.

**May/June 2024**

**13.** In the context of Payment Gateways, algorithms are employed to secure data. Which concept describes asymmetric cryptography?
(A) It employs different keys for encryption and decryption to mask data securely.
(B) It uses a single identical key for both encrypting and decrypting data transmissions.
(C) It relies on physically protecting the network infrastructure rather than modifying the data.
(D) It completely replaces sensitive data with temporary dynamic tokens rather than encrypting it.

**Oct/Nov 2018**

**14.** Stored Value Cards, or prepaid cards, differ fundamentally from traditional debit cards. Which conceptual attribute is unique to Stored Value Cards?

Click Here to Buy book on Amazon

Key Certificates. User PKCs are required for every individual at the gateway or branch level, such as verifiers and authorizers. Server signing PKCs enable the SFMS server to digitally sign data, while server encryption PKCs allow for the secure encryption of information. Additionally, secure server PKCs are utilized to restrict access to the system through encrypted HTTPS modes.

**99.** (B) n98 — Proprietary Returns & Statements
In the Structured Financial Messaging System, specific alphanumeric codes are used to identify non-standard or proprietary message types. The code "n98" is designated for proprietary returns and statements, which are often used for reporting data that does not fit into standard financial message formats. This allows banks and the central bank to exchange various statistical or administrative reports while still benefiting from the secure and authenticated transmission infrastructure of SFMS.

**100.** (C) Off-line Servers (Thick Clients)
A bank branch facing network issues should utilize Off-line Servers, also known as Thick Clients, to maintain operational continuity. These systems are equipped with specialized SFMS software that allows users to create, verify, and authorize financial messages locally without a continuous connection to the main Branch Server. Once the network link is restored, the prepared messages can be synchronized and transmitted, ensuring that branch productivity is not hindered by connectivity gaps.

**101.** (A) IFN 298 G Series
When a bank branch needs to securely relay information regarding government account transactions to its central reporting office, it uses the IFN 298 G series message format. This specific Structured Financial Messaging System format is designed to handle the structured data requirements associated with government banking. By using the intra-bank SFMS network, the branch ensures that these critical reports are delivered with the necessary authentication and integrity for official record-keeping.

**102.** (A) It switches Intra-Bank messages between Branch Servers and forwards Inter-Bank messages to the Hub.
Within the Structured Financial Messaging System architecture, the Bank Gateway serves as a critical intermediary. It is responsible for routing intra-bank messages between different branch servers within the same institution. Additionally, it handles outgoing inter-bank messages by forwarding them to the centralized SFMS Hub located at IDRBT. This dual role ensures that both internal and external financial communications are directed to their correct destinations with the appropriate security protocols.

**103.** (D) (I), (II), (III), and (IV)
SFMS utilizes a variety of standardized IFN message formats to handle different types of intra-bank transactions. For instance, the 100 series is used for customer telegraphic transfers, while the 110 series manages demand draft messages. Inter-bank fund transfers typically utilize the 200 series, and messages related to bank guarantees are processed through the 760 and 769 formats. These structured codes ensure that all participants understand the specific nature of each transmitted message.

**104.** (B) Copies of messages are permanently stored on On-line terminals to allow offline viewing.
On-line terminals in the SFMS environment function as thin clients, using a standard web browser to access the Branch Server. Because these terminals do not have specialized SFMS software installed locally, they do not store copies of messages permanently. For offline capabilities such as viewing or processing messages without an active server connection, branches must use Thick Clients or Off-line Servers, which are specifically designed to store and manage local data.

NODIA

**105.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
The Structured Financial Messaging System is a form of Electronic Data Interchange because it facilitates the exchange of financial information using highly structured formats. These formats are determined by a dedicated Working Group on Message Standards, which publishes the precise layouts and rules that all participants must follow.

(A) NFC is a technology designed to transmit data over distances exceeding 10 kilometers for banking.
(B) NFC is primarily used to process electronic checks directly through magnetic stripe readers.
(C) NFC enables two nearby devices, such as a phone and terminal, to communicate with each other.
(D) NFC eliminates the need for smart devices, making it exclusively reliant on the use of paper money.

**Oct/Nov 2021**

**22.** In a credit card payment, a standard form called the "CHARGE SLIP" or "SALE DRAFT" is completed. How many copies of this draft are typically generated?
(A) 1
(B) 2
(C) 3
(D) 4

**May/June 2010**

**23.** The utility of a credit card is derived from its revolving nature. Which of the following best explains this concept?
(A) The cardholder's funds are immediately debited from their deposit account on a recurring daily basis.
(B) The total value on the card decreases with usage but can be replenished by transferring cash at an ATM.
(C) The cardholder uses the sanctioned limit, which then automatically renews upon repayment of dues.
(D) The card can be utilized interchangeably at various merchant locations without any need for validation.

**Oct/Nov 2024**

**24.** Identify the correct statement concerning reloadable and disposable smart cards.
(A) Disposable cards can have their value replenished by paying cash at a special terminal on campus.
(B) Reloadable cards come with a specific value and must be discarded once the initial value is exhausted.
(C) Reloadable cards are exclusively designed to operate within closed system institutional environments.
(D) Reloadable cards can have their value replenished by the consumer at a special terminal or ATM.

**May/June 2017**

**25.** RuPay was launched to provide a domestic, open loop system in India. What conceptual feature characterizes an open loop system?
(A) Cards are restricted to specific local environments like mass-transit systems or university campuses.
(B) Cards are accepted universally across various issuers and merchants for general consumer purchases.
(C) Transactions are processed internally without any requirement for international currency convertibility.
(D) The card value is completely depleted and the physical card is discarded once funds are exhausted.

**Oct/Nov 2019**

**26.** Which of the following best defines a Point of Sale (POS) terminal?
(A) An online platform that provides a secure connection to process transactions between an e-commerce entity and a merchant.
(B) A self-service machine that primarily duplicates the services of a live bank teller for deposits and withdrawals.
(C) A centralized database vault that stores the relationship between sensitive card values and their encrypted tokens.
(D) An electronic device used to process card payments at retail locations through a combination of software and hardware.

**May/June 2025**

**27.** Which of the following statements about the acceptance of RuPay cards is correct?
(A) The NPCI maintains ties with Discover Financial to enable international acceptance for RuPay cards.
(B) RuPay cards are accepted exclusively at ATMs and cannot be used for any online e-commerce transactions.
(C) RuPay transactions are predominantly international, with 90% of debit card transactions occurring abroad.
(D) RuPay chip cards are primarily signature-based rather than PIN-based to ensure rapid retail processing.

Downloaded from www.pdf.tube

1. Launch of mobile payment solutions Android Pay and Apple Pay.
2. Motioncode (Dynamic CVV) technology was introduced.
3. RBI mandated card tokenization for online transactions.
4. Open system VISA cards used widely during the Olympics.

(A) P-4, Q-1, R-2, S-3
(B) P-1, Q-4, R-3, S-2
(C) P-2, Q-3, R-4, S-1
(D) P-4, Q-2, R-1, S-3

**Oct/Nov 2016**

**84.** Consider the following statements about the RuPay network:

I RuPay chip cards use an embedded microprocessor containing PIN-based information.
II RuPay maintains an agreement with Discover Financial (DFS) for international acceptance.
III NCMC debit cards on the RuPay platform are exclusively restricted to Metro train services.

Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

**May/June 2011**

**85.** Consider the following statements regarding card technologies:

I The conventional magnetic stripe on ATM cards stores information across 4 tracks.
II Smart cards strictly possess less data storage capacity than magnetic stripe cards.

Which of the following options is correct?
(A) Only (I) is correct.
(B) Only (II) is correct.
(C) Both (I) and (II) are correct.
(D) Both (I) and (II) are incorrect.

**Oct/Nov 2011**

**86.** Match the security codes in List I with their appropriate use case in List II.

List I: (Security Codes)
P. CVC1
Q. CVC2
R. iCVV
S. Motioncode

List II: (Use Case)
1. Electronic code supplied by contactless cards and chip cards.
2. A dynamic code that automatically refreshes every hour.
3. Encoded on track two for card present transactions.
4. Sought by merchants for card not present transactions via Internet.

(A) P-3, Q-4, R-1, S-2
(B) P-4, Q-3, R-2, S-1
(C) P-1, Q-2, R-4, S-3
(D) P-3, Q-1, R-4, S-2

**May/June 2024**

**87.** Consider the following statements comparing credit and debit cards:

I A credit card user accesses a line of credit.
II A debit card user must maintain an account and balance.
III Payment for a credit card is immediate by debiting the holder's account.
IV Credit card payments can be made from any other bank account.

Which of the above statement(s) is/are correct?
(A) (I), (II), and (IV)
(B) (I), (III), and (IV)
(C) (II), (III), and (IV)
(D) (I), (II), and (III)

NODIA

**Oct/Nov 2021**

**88.** Match the credit card operational terms in List I with their explanations in List II.

List I: (Operational Terms)
P. Floor Limit
Q. Card Limit
R. Hot List
S. Billing Cycle

List II: (Explanations)
1. Maximum amount a cardholder can spend, restored upon payment.
2. Discretionary per-transaction limit fixed by the acquirer.
3. Database of lost, stolen, or defaulting cards to retrieve them.
4. Periodical interval at which the issuer sends a transaction statement.

(A) P-2, Q-1, R-3, S-4
(B) P-1, Q-2, R-4, S-3
(C) P-3, Q-4, R-1, S-2
(D) P-4, Q-3, R-2, S-1

# STUDYING FROM PDFs?

# THINK AGAIN.

If you are studying only from PDFs,
you are wasting valuable time.

Research shows that learning from

**PRINTED BOOKS** has up to

**4× HIGHER RETENTION**

than studying from screens.

**PRINT BOOK = BETTER MEMORY**

**PDF = LOWER RETENTION**

Those who study from **PRINTED BOOKS**
move **AHEAD.**

Others are left **BEHIND**
in competition.

In competitive exams,
being average is not enough.

## STAY ONE STEP AHEAD.

(C) It can be utilized by tourists or children who do not possess a formal bank account.
(D) It makes the cost of financial operation for the bank much cheaper compared to a magnetic stripe card.

**Oct/Nov 2022**

**36.** Following the RBI directive effective from 1 July 2022, where does the ultimate responsibility for card tokenisation services rest?
(A) The authorised card networks like VISA, MasterCard, and RuPay.
(B) The e-commerce merchants such as Amazon and Flipkart.
(C) The third-party payment gateways like BillDesk and PayUMoney.
(D) The individual consumers conducting the online transactions.

**May/June 2005**

**37.** Identify the incorrect statement regarding credit card limits.
(A) The Floor Limit is an overall spending limit given to the cardholder, which is billed once a month.
(B) Floor limit is a per-transaction limit fixed by the acquirer.
(C) Floor limit gives the merchant establishment some discretion to accept cards in payment.
(D) The Card Limit given to a cardholder is automatically restored upon payment of the bill.

**Oct/Nov 2020**

**38.** Which of the following is NOT an example of a popular payment gateway operating in India?
(A) CC Avenue
(B) PayUMoney
(C) BillDesk
(D) Discover Financial

**May/June 2020**

**39.** Which scenario serves as the best example of an "Electronic Purse" or "Electronic Wallet" in an open system?
(A) A card issued by a university exclusively for purchasing books and photocopying within its campus.
(B) A prepaid transit card used strictly for the local subway system.
(C) A dedicated phone card designed exclusively to access a specific telecom operator's network.
(D) Cards issued by separate banks that are mutually acceptable across over 1500 different merchants.

**Oct/Nov 2006**

**40.** Identify the incorrect statement about Point of Sale (POS) terminals and electronic funds transfer.
(A) POS terminals can check whether the funds in a customer's bank account are sufficient.
(B) EFTPOS is an electronic payment system involving funds transfers based on payment cards at retail locations.
(C) Small merchants may be required to pay rent for the POS terminal alongside per-transaction fees.
(D) Despite advanced POS technology, systems remain invulnerable to dishonest cashiers entering lower quantities to profit.

**May/June 2023**

**41.** Arrange the following steps in the continuous cycle of a credit card transaction in the correct chronological order:
I The bank sends notice to the customer to make payment.
II The cardholder makes a purchase from the authorized merchant.
III The cardholder makes payment to the bank.
IV The merchant submits a claim to the bank, and the bank pays the merchant.
(A) (I), (II), (III), (IV)
(B) (II), (IV), (I), (III)
(C) (II), (I), (IV), (III)
(D) (IV), (II), (I), (III)

**May/June 2006**

**42.** Identify the incorrect statement concerning CVV or CSC numbers and their limitations.
(A) Phishing scams trick cardholders into entering the CSC on a fraudulent or malicious website.
(B) The Motioncode system introduced in 2016 addresses CSC limitations by refreshing the code.
(C) CVV provides absolute protection against scammers who have already acquired the card number.
(D) Phishing has reduced the effectiveness of the CSC as a real-world anti-fraud security device.

Click Here to Buy book on Amazon

Oct/Nov 2024

**43.** The Reserve Bank of India has mandated card tokenization features. Which of the following does NOT accurately describe the tokenization framework?
(A) Tokens will be issued as 16-digit numbers mimicking standard card details.
(B) A single unique token is universally issued per card to be utilized across all merchants.
(C) A 'token reference number' is created against each token and stored by the merchant.
(D) Customers do not need to memorize or remember their newly generated token details.

May/June 2011

**44.** Which of the following is NOT mentioned as a manufacturer of smart cards?
(A) TSMC
(B) NXP
(C) Global founders
(D) DFS

Oct/Nov 2021

**45.** For mobile payments like Android Pay and Apple Pay to go fully mainstream, what technology must first become universally adopted by devices?
(A) Secure Socket Layer (SSL)
(B) Electronic Funds Transfer at Point of Sale (EFTPOS)
(C) Near Field Communication (NFC)
(D) Card on File Tokenization (CoFT)

May/June 2015

**46.** Which of the following statements is incorrect when comparing credit and debit cards?
(A) A debit card utilizes funds up to the total available balance in the user's personal bank account.
(B) A credit card holder must maintain a savings account and balance with the issuing bank.
(C) A credit card allows the user to access a bank-sanctioned line of credit for general expenditures.
(D) Debit card payments are made immediately by debiting the user's account for the transaction amount.

Oct/Nov 2008

**47.** The real-world effectiveness of the CVV (CSC) as an anti-fraud device is severely diminished by which primary vulnerability?
(A) The physical duplication of the magnetic stripe's second track during a swipe.
(B) Phishing scams that trick the cardholder into entering the CSC on a fake website.
(C) The automatic hourly refreshment of the code which disrupts typical online processing.
(D) The rejection of 4-digit numeric codes by older, legacy payment gateway systems.

May/June 2024

**48.** Which of the following statements about Automated Teller Machines (ATMs) is incorrect?
(A) White label ATMs are ATMs managed by non-banking entities.
(B) The prospect of a truly cashless society was fully realized by the deployment of the first-generation ATMs alone.
(C) ATMs allowed 24-hour access and effectively became mini-branches extending financial territories.
(D) Prism Payment Services and Indicash are examples of entities that manage white label ATMs.

NODIA

May/June 2007

**49.** Which of the following transactions is NOT covered by the mandatory card tokenisation framework directed by the RBI?
(A) International transactions processed across foreign e-commerce portals.
(B) Domestic transactions processed via MasterCard.
(C) Online transactions requiring the saving of card details by Indian sellers.
(D) Tokenized purchases authenticated via Visa and RuPay networks.

Oct/Nov 2006

**50.** There are several types of security codes utilized in payment cards. Which of the following is NOT a recognized security code type?
(A) CVC1
(B) iCVV
(C) CoFT
(D) CVC2

May/June 2006

**51.** Under the CoFT framework, a token serves as a replacement for actual card details. What provides the best explanation of a token's uniqueness?

(A) A token is uniquely generated strictly for a single specific monetary transaction value.
(B) A token is unique to the device, irrespective of the card or specific merchant used.
(C) A single 16-digit token is assigned to a consumer across all devices and platforms.
(D) A token is unique for a combination of the card, token requestor, and the device used.

**Oct/Nov 2012**

**52.** Which statement regarding RuPay cards is incorrect?
(A) RuPay is an Indian domestic card scheme conceived and launched by the NPCI.
(B) NPCI rolled out chip cards with embedded microprocessors for high-security PIN-based transactions.
(C) RuPay cards are accepted online on thousands of e-commerce websites using the same PIN used for ATM transactions.
(D) NPCI has completely avoided integrating EMV chip technology to ensure RuPay cards remain uniquely signature-based.

**May/June 2013**

**53.** Which of the following is NOT a defined step in the continuous cycle of a credit card transaction?
(A) The cardholder makes a purchase from an authorized merchant.
(B) The merchant submits a claim to the bank.
(C) The merchant directly demands monthly interest payments from the cardholder for the sold goods.
(D) The bank sends a notice to the customer to make payment.

**Oct/Nov 2013**

**54.** Despite upgrading POS terminals, what is the most critical vulnerability affecting ATM card transactions relying on magnetic stripes?
(A) They are incapable of initiating electronic funds transfers.
(B) They mandate the physical presence of a teller to approve withdrawals.
(C) They remain highly susceptible to skimming and cloning frauds.
(D) They automatically delete stored value upon insertion into an ATM.

NODIA

**May/June 2008**

**55.** Which of the following is NOT a function typically performed by a Point of Sale (POS) terminal?
(A) Issues and manages a dynamic token vault for all retail merchant accounts.
(B) Reads the information stored on a customer's physical credit or debit card.
(C) Checks whether the funds in the customer's bank account are sufficient.
(D) Records the details of the transaction and prints a customer receipt.

**Oct/Nov 2014**

**56.** Which statement about closed and open stored value cards is incorrect?
(A) Phone cards and subway cards are primary examples of open system stored value cards.
(B) In an open system, the cards of several issuers are mutually acceptable across numerous merchants.
(C) The 1996 Olympics utilized an open system where VISA cards were accepted by over 1500 merchants.
(D) A closed system stored value card can only be used at specified locations, such as mass-transit systems or university campuses.

**May/June 2014**

**57.** ATMs significantly transformed modern banking operations. What provides the best explanation for how ATMs "began to blur the divisions between banks"?
(A) By networking institutions into a system linking people far beyond physical buildings.
(B) By standardizing the physical design of bank branches across different financial entities.
(C) By exclusively dispensing a uniform international currency regardless of the bank's origin.
(D) By allowing merchants to act as acquiring banks and issue their own branded credit cards.

**Oct/Nov 2015**

**58.** Identify the incorrect statement regarding the RBI mandate on Card Tokenization.
(A) Users are completely exempt from requesting a new token even if a fraud is detected against an active token.
(B) Sensitive credit or debit card information cannot be stored by merchants while

network a token generation fee per transaction.

Which of the above statement(s) is/are correct?
(A) (I), (II), and (IV)
(B) (I), (II), and (III)
(C) (II), (III), and (IV)
(D) (I), (III), and (IV)

**Oct/Nov 2023**

**72.** Match the following entities/concepts in List I with their descriptions in List II.

List I: (Entities/Concepts)
P. VISA and MasterCard
Q. American Express
R. NPCI
S. Reserve Bank of India (RBI)

List II: (Descriptions)
1. Domestic card scheme creator (RuPay).
2. Uses a 4-digit numeric code for CVV.
3. Mandated tokenization to secure online transactions.
4. Fixes the issuer's portion of the commission.

(A) P-4, Q-2, R-1, S-3
(B) P-2, Q-4, R-3, S-1
(C) P-1, Q-3, R-2, S-4
(D) P-4, Q-1, R-2, S-3

**May/June 2010**

**73.** Consider the following statements about ATM upgrades in India:
I RBI set a target for banks to upgrade all ATMs by September 2017 to process EMV chip and PIN cards.
II NPCI continues to actively route all Magstripe card transactions to encourage legacy infrastructure usage.

Which of the following options is correct?
(A) Only (I) is correct.
(B) Only (II) is correct.
(C) Both (I) and (II) are correct.
(D) Both (I) and (II) are incorrect.

**Oct/Nov 2005**

**74.** Identify the correct pair matching a smart card component or technology with its definition.
(A) Magnetic Stripe - Embedded microprocessor circuit performing calculations.
(B) Interchange - The cost of manufacturing a silicon chip.
(C) Closed System Card - Usable only in specified locations like mass-transit.
(D) Stored Value Card - Requires a mandatory checking account.

**May/June 2005**

**75.** Consider the following statements regarding the advantages of smart cards:
I They have active anti-fraud capabilities and high data security.
II They can perform complex decision-making tasks like mutual authentication.
III They may perform offline validation natively on the card.
IV They strictly require the user to possess a regular bank deposit account.

Which of the above statement(s) is/are correct?
(A) (I), (II), and (IV)
(B) (I), (II), and (III)
(C) (II), (III), and (IV)
(D) (I), (III), and (IV)

**Oct/Nov 2007**

**76.** Match the terms in List I with their respective descriptions in List II.

List I: (Terms)
P. Acquirer
Q. Issuer
R. Interchange
S. Charge Back

List II: (Descriptions)
1. The commission earned by the acquiring bank.
2. The bank that has an agreement with the merchant.
3. Transactions authorized but later disputed by the cardholder.
4. The bank that sends a transaction statement to the cardholder.

(A) P-2, Q-4, R-1, S-3
(B) P-4, Q-2, R-3, S-1
(C) P-1, Q-3, R-2, S-4
(D) P-2, Q-1, R-4, S-3

**May/June 2012**

**77.** Consider the following statements regarding Payment Gateways:
I A payment gateway provides a secure connection to carry out transactions between an e-commerce entity and a merchant account.
II The payment gateway verifies, accepts, or declines transactions in real time on a merchant's behalf.
III Data encryption uses algorithms to ensure

Downloaded from www.pdf.tube

May/June 2020

**65.** Identify the correct pair representing a card brand and its associated CVV code length.
(A) VISA - 3 digit numeric code
(B) Discover - 4 digit numeric code
(C) American Express - 3 digit numeric code
(D) MasterCard - 5 digit numeric code

Oct/Nov 2020

**66.** Consider the following statements concerning CVV and its limitations:
I CVC1 is retrieved automatically during a card-present transaction.
II CVC2 is often sought by merchants for card-not-present transactions.
III The CSC offers robust, unbreakable protection against Phishing scams.
IV The Motioncode system addresses limitations by refreshing the CVV code every hour.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (IV)
(B) (II), (III), and (IV)
(C) (I), (II), and (III)
(D) (I), (III), and (IV)

May/June 2021

**67.** Arrange the following steps involved in an e-commerce transaction in chronological order:
I The seller's bank forwards transaction information to the card-issuing bank.
II The customer purchases an item and enters card details.
III The bank verifies details, approves the transaction, and sends information back to the seller's bank.
IV The payment gateway forwards transaction information to the seller's bank.
(A) (II), (IV), (I), (III)
(B) (II), (I), (IV), (III)
(C) (IV), (II), (III), (I)
(D) (II), (III), (I), (IV)

Oct/Nov 2011

**68.** Consider the following statements:
I A cardholder defaulting in payment or exceeding the limit results in the issuer placing the card in the hot list.
II A credit card allows the user to access a revolving line of credit that renews automatically upon repayment.
Which of the following options is correct?
(A) Only (I) is correct.
(B) Only (II) is correct.
(C) Both (I) and (II) are correct.
(D) Both (I) and (II) are incorrect.

NODIA

May/June 2022

**69.** Consider the following statements regarding Stored Value Cards:
I They are also known as prepaid cards or value-added cards.
II The consumer pays a bank for the card loaded with the value.
III Funds are directly debited from the cards and transferred to the vendor's terminal.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

Oct/Nov 2022

**70.** Match the tokenization components in List I with their properties in List II.
List I: (Components)
P. Token Vault
Q. CoFT
R. Token Reference Number
S. Authorized Card Networks
List II: (Properties)
1. The entities ultimately responsible for tokenisation services.
2. Identifiers created and stored by merchants against each token.
3. Database storing the relationship between the sensitive value and token.
4. Replacement of actual card details with a unique alternate code.
(A) P-3, Q-4, R-2, S-1
(B) P-4, Q-3, R-1, S-2
(C) P-2, Q-1, R-4, S-3
(D) P-3, Q-2, R-4, S-1

May/June 2023

**71.** Consider the following statements regarding the consumer experience under Card Tokenization:
I Consumers will not be able to directly view or know their token details.
II Tokens are generated as distinct 16-digit numbers.
III Banks will create portals allowing cardholders to manage or delete tokens.
IV Consumers must actively pay the card

Oct/Nov 2007

**28.** Electronic funds transfer at point of sale (EFTPOS) is highly popular and accounts for about 60% of all retail transactions in which of the following countries?
(A) New Zealand
(B) India
(C) United States of America
(D) United Kingdom

May/June 2015

**29.** Identify the correct statement regarding the application cycle of credit cards.
(A) The bank sends notice to the cardholder to pay for goods before the merchant submits a claim to the bank.
(B) The cardholder makes payment directly to the merchant, effectively bypassing any bank involvement.
(C) The merchant submits a claim to the bank, which then pays the merchant for the goods or services.
(D) The cardholder completes the purchase and immediately reimburses the acquiring bank for the amount.

Oct/Nov 2013

**30.** Smart cards are engineered to overcome the limitations of magnetic stripe cards. What is a primary conceptual advantage of a smart card over a magnetic stripe card?
(A) It eliminates the need for any form of terminal infrastructure for transaction processing.
(B) It standardizes the commission interchange rate across all acquiring banks.
(C) It restricts usage to closed system environments like university campuses.
(D) It performs complex decision-making tasks, including mutual authentication to reduce fraud.

May/June 2008

**31.** Identify the incorrect statement related to Data Encryption in payment gateways.
(A) Card details get encrypted using the payment gateway's public key.
(B) Encrypted details can only be decrypted by the payment gateway's private key.
(C) Asymmetric cryptography uses the exact same key for both encryption and decryption.
(D) The algorithm ensures unauthorized parties cannot decrypt the data during network transmission.

Oct/Nov 2012

**32.** Which of the following entities does NOT issue tokens under the Card Tokenization mandate?
(A) Visa
(B) Individual e-commerce merchants (e.g., Zomato, Flipkart)
(C) MasterCard
(D) RuPay

May/June 2013

**33.** Identify the incorrect statement regarding the advantages of smart cards.
(A) Smart cards can perform offline validation natively on the card itself.
(B) Smart cards are highly vulnerable because their validation must always be conducted online.
(C) The cost of financial operation for the bank is much cheaper compared to magnetic stripe cards.
(D) Smartcards can incorporate biometrics such as fingerprints to firmly connect the identity of the cardholder to the card.

Oct/Nov 2009

**34.** Fraud prevention is a main motivator for the Secure Electronic Transaction (SET) protocol. What is the primary method SET employs to protect consumer privacy?
(A) It mandates the use of physical smart card readers attached to the customer's home computer.
(B) It replaces the card details with a 16-digit token managed by a centralized token vault.
(C) It requires merchants to verify biometric data through a centralized national database system.
(D) It encrypts payment information so only the bank can see details, blocking the merchant.

May/June 2016

**35.** Which of the following is NOT categorized as an advantage of a smart card?
(A) It necessitates mandatory online validation for every single transaction due to lack of an internal chip.
(B) It provides active anti-fraud capabilities and high data security.

Click Here to Buy book on Amazon

unauthorized parties cannot decrypt transmitted data.

Which of the above statement(s) is/are correct?

(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

**Oct/Nov 2025**

**78.** Match the technologies/terminals in List I with their functionality in List II.

List I: (Technologies/Terminals)

P. POS Terminal
Q. NFC
R. NCMC
S. EFTPOS

List II: (Functionality)

1. Contactless technology enabling devices in close proximity to communicate.
2. Retail electronic device checking funds and transferring money.
3. Electronic payment system highly popular in Australia and New Zealand.
4. Stored value contactless smartcard used in Metro trains and buses.

(A) P-2, Q-1, R-4, S-3
(B) P-1, Q-2, R-3, S-4
(C) P-4, Q-3, R-2, S-1
(D) P-2, Q-4, R-1, S-3

**May/June 2016**

**79.** Consider the following statements regarding the consumer aspect of tokenization:

I Consumers must pay a mandatory fee to the banks to generate tokens for online domestic transactions.
II Card tokenization applies strictly to international transactions, exempting domestic purchases.

Which of the following options is correct?

(A) Only (I) is correct.
(B) Only (II) is correct.
(C) Both (I) and (II) are correct.
(D) Both (I) and (II) are incorrect.

**Oct/Nov 2010**

**80.** Identify the incorrect pair relating to Card Tokenization mandates.

(A) Identifier for Merchants - Token reference number.
(B) Format of Token - 16-digit number.
(C) Issuer of Tokens - Credit and Debit card networks.
(D) Storage capability - Merchants allowed to store Card CVV post-July 2022.

**May/June 2009**

**81.** Consider the following statements regarding the Secure Electronic Transaction (SET) protocol:

I SET was developed by Visa and MasterCard.
II SET prevents merchants from accessing sensitive credit card information.
III SET utilizes customer digital signatures to maintain confidentiality and authenticity.
IV SET mandates that all merchants install customized biometrics hardware.

Which of the above statement(s) is/are correct?

(A) (I), (II), and (III)
(B) (I), (II), and (IV)
(C) (II), (III), and (IV)
(D) (I), (III), and (IV)

**Oct/Nov 2009**

**82.** Match the security mechanisms in List I with their functions in List II.

List I: (Security Mechanisms)

P. Payment Gateway
Q. Data Encryption
R. SSL
S. SET

List II: (Functions)

1. Uses digital signatures to block card details from merchants.
2. An online platform providing secure connection for transaction processing.
3. Standard cryptographic protocol establishing an encrypted link via web server.
4. Uses public and private keys (symmetric/asymmetric) to mask data.

(A) P-2, Q-4, R-3, S-1
(B) P-4, Q-2, R-1, S-3
(C) P-3, Q-1, R-4, S-2
(D) P-2, Q-3, R-4, S-1

**May/June 2025**

**83.** Match the years in List I with the corresponding industry event in List II.

List I: (Years)

P. 1996
Q. 2015
R. 2016
S. 2022

List II: (Industry Events)

NODIA

processing online transactions.
(C) Authorised card networks are ultimately responsible for the card tokenisation services rendered.
(D) E-commerce platforms like Amazon and Flipkart are instructed to delete earlier stored card information.

**May/June 2017**

**59.** What represents the primary utility of a credit card for a consumer?
(A) Earning an interchange fee equivalent to 2% to 3.5% for every retail transaction.
(B) Generating a dynamic CVV code every hour to track personal expenditures.
(C) The ability to buy goods and services without paying for them immediately.
(D) Bypassing the need for a PIN code at an automated teller machine terminal.

**Oct/Nov 2017**

**60.** Which of the following is NOT a correct security practice concerning the CVV number?
(A) Providing the CVV to an online merchant to prove physical possession of the card.
(B) Entering the CVV number directly into an ATM to authorize a cash advance.
(C) Refraining from entering the card PIN when asked to provide the CVV online.
(D) Relying on dynamic CVV technology (Motioncode) to refresh the security code.

**May/June 2018**

**61.** Match the organizations in List I with their respective categories in List II.
List I: (Organizations)
P. CC Avenue
Q. TSMC
R. Discover Financial Services (DFS)
S. Indicash
List II: (Categories)
1. White Label ATM provider.
2. International network tied with RuPay.
3. Payment Gateway.
4. Smart card manufacturer.
(A) P-3, Q-4, R-2, S-1
(B) P-4, Q-3, R-1, S-2
(C) P-2, Q-1, R-4, S-3
(D) P-3, Q-2, R-4, S-1

**Oct/Nov 2018**

**62.** Consider the following statements about online security protocols:
I Secure Socket Layer (SSL) uses a padlock symbol and an https prefix to authenticate website identity.
II Transport Layer Security (TLS) is now considered outdated and has been replaced by SSL.
Which of the following options is correct?
(A) Only (I) is correct.
(B) Only (II) is correct.
(C) Both (I) and (II) are correct.
(D) Both (I) and (II) are incorrect.

**May/June 2019**

**63.** Match the card types in List I with their specific characteristics in List II.
List I: (Card Types)
P. Credit Card
Q. Debit Card
R. Smart Card
S. Closed Stored Value Card
List II: (Characteristics)
1. Payment made immediately by debiting a deposit account.
2. Can only be used in specified locations like mass-transit.
3. Features an embedded computer chip for storing data and calculations.
4. Provides a revolving consumer loan up to a sanctioned limit.
(A) P-4, Q-3, R-1, S-2
(B) P-4, Q-1, R-3, S-2
(C) P-1, Q-4, R-2, S-3
(D) P-3, Q-2, R-4, S-1

**Oct/Nov 2019**

**64.** Consider the following statements concerning Card Tokenization rules:
I Merchants such as Zomato and Amazon must delete stored card information.
II A single card generates multiple distinct tokens if used across different merchants.
III Consumers who do not want to save card details can manually enter details for a one-time purchase.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

Downloaded from www.pdf.tube

May/June 2015

**89.** Consider the following statements about the transaction process:

I The cardholder is generally given two weeks' time to pay the billed amount.

II The acquirer pays the amount of the sale draft to the merchant less his commission.

III The commission earned by the acquirer is strictly retained and never shared with the issuing bank.

Which of the above statement(s) is/are correct?

(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

Oct/Nov 2012

**90.** Identify the incorrect pair linking an Indian payment gateway to its name.

(A) Payment Gateway - NXP
(B) Payment Gateway - CC Avenue
(C) Payment Gateway - Instamojo
(D) Payment Gateway - BillDesk

May/June 2008

**91.** In the following questions, a statement of Assertion (A) is followed by a statement of Reason (R). Choose the correct option:

Assertion (A): A debit card requires the customer to maintain an account and available balance.

Reason (R): The use of a debit card results in immediate payment by debiting the holder's personal deposit account.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Oct/Nov 2008

**92.** Based on the case of Mr. Sharma, an electronics showroom operator, answer the following question: If a transaction processed by Mr. Sharma is later disputed by the cardholder, and the issuing bank claims back the amount from the acquirer after satisfying itself about the dispute, this process is termed:

(A) Skimming
(B) Motioncode activation
(C) Charge Back
(D) Card on File reversal

May/June 2013

**93.** Consider the following statements regarding security codes and their mapping:

I CVC1 or CVV1 is encoded on track two of the magnetic stripe.

II CVC1 is primarily utilized for card present transactions.

III A major limitation of CVC1 is that it remains valid if the entire magnetic stripe is copied.

IV CVC2 is often required by merchants for telephone or Internet transactions.

V iCVV or dynamic CVV are electronically generated codes supplied strictly by magnetic stripes.

Which of the above statement(s) is/are correct?

(A) (I), (II), (III), and (IV) only
(B) (II), (III), (IV), and (V) only
(C) (I), (II), (IV), and (V) only
(D) All (I), (II), (III), (IV), and (V)

Oct/Nov 2013

**94.** Based on the case of Miss Verma shopping online, answer the following question: The 3-digit CVV code on the reverse of the card, typically sought by merchants for card-not-present internet transactions, is technically referred to as:

(A) CVC1
(B) iCVV
(C) CVC2
(D) NFC code

May/June 2007

**95.** In the following questions, a statement of Assertion (A) is followed by a statement of Reason (R). Choose the correct option:

Assertion (A): Data encryption utilizes algorithms to securely transmit data through networks.

Reason (R): Symmetric cryptography masks data by using completely different keys for encryption and decryption.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.

NODIA

numeric code used for card-not-present transactions, such as online shopping, to ensure the person has the physical card in hand.

**9.** (B) It is a disputed transaction where the bank claims back the payment amount from the acquirer.
A chargeback occurs when a cardholder or the issuing bank disputes a transaction after it has been authorized. The bank then claims back the payment amount from the acquirer to resolve the dispute. This process protects consumers against unauthorized charges or failed service delivery, shifting the financial responsibility back to the merchant until the conflict is formally settled.

**10.** (C) 2016
Motioncode technology was introduced in the year 2016 to enhance the security of online transactions. This innovation features a dynamic card verification value that refreshes automatically at regular intervals, typically every hour. By replacing the static security code with a constantly changing one, the system effectively renders captured card data useless for future fraudulent activities by unauthorized third parties.

**11.** (B) Consumers who choose not to have their card details stored do not require to follow tokenisation for one-time purchases.
In the Indian context, the card tokenization mandate applies primarily to domestic e-commerce transactions where merchants intend to store card details. Consumers who prefer not to have their card information saved can opt out of tokenization. These users may still perform one-time purchases by manually entering their card details for each transaction, maintaining flexibility while ensuring higher data security.

**12.** (C) The replacement of actual card details with a unique alternate code to securely process online transactions.
Card tokenization is a security process where actual sensitive card details are replaced with a unique alternate code called a token. This token allows online transactions to be processed securely without exposing the real card number to merchants or third-party gateways. By using these identifiers, the risk of data breaches and fraudulent use of stolen card information is significantly minimized.

**13.** (A) It employs different keys for encryption and decryption to mask data securely.
Asymmetric cryptography is a security concept used to protect data during transmission by employing a pair of different keys. One key is used for encrypting the information, while a separate, mathematically related key is required for decryption. This method ensures that even if the encrypted data is intercepted, only the authorized recipient possessing the private key can access the original content.

**14.** (C) They carry monetary value and transactions do not necessitate the use of a formal bank account.
Stored value cards carry a pre-loaded monetary value directly on the card itself, distinguishing them from traditional debit or credit cards. Transactions using these cards do not necessitate the use of a formal bank account for authorization at the point of sale. This feature makes them highly accessible for diverse users, including children or individuals without standard banking relationships.

**15.** (D) The payment gateway forwards the transaction information from the e-commerce checkout to the seller's bank.
During an e-commerce transaction, the payment gateway acts as a secure intermediary between the checkout page and the financial networks. It captures the customer's card details and forwards the transaction information to the merchant's acquiring bank. This step is essential for initiating the authorization process, where the merchant's bank communicates with the issuer to verify funds and approve the purchase.

**16.** (A) A per-transaction limit where merchants may accept cards without prior authorization.
A floor limit is a specific per-transaction amount established by the acquiring bank. For transactions falling below this limit, merchants may have the discretion to accept the payment card without seeking prior authorization from the issuer. This mechanism helps expedite retail processing for small-value purchases while maintaining a balance between operational

Click Here to Buy book on Amazon

cyberattacks and payment fraud.
IV The token concept is entirely new to India and never utilized before 2022.
V Apple Pay and Google Pay operate on a tokenization system.

Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (IV) only
(B) (I), (III), (IV), and (V) only
(C) (I), (II), (III), and (V) only
(D) All (I), (II), (III), (IV), and (V)

**May/June 2019**

**103.** Based on the case of Mr. Sharma, an electronics showroom operator, answer the following question: When the acquiring bank processes Mr. Sharma's sales drafts, it deducts a commission ranging from 2% to 3.5%. What is this commission earned by the acquirer called?
(A) Tokenization fee
(B) Interchange
(C) Charge Back penalty
(D) Floor discount

**Oct/Nov 2019**

**104.** In the following questions, a statement of Assertion (A) is followed by a statement of Reason (R). Choose the correct option:
Assertion (A): The SET protocol blocks the details of credit card information from being seen by merchants.
Reason (R): SET encrypts payment information so that only the involved bank can access and view the sensitive details.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2020**

**105.** Based on the case of Miss Verma shopping online, answer the following question: If a card is equipped with technology that automatically refreshes the CVV code every hour to make captured data useless, this technology is called:
(A) Secure Socket Layer (SSL)
(B) Token Vault
(C) Motioncode (Dynamic CVV)
(D) EMV Chip and PIN

**Oct/Nov 2020**

**106.** Consider the following statements regarding ATM technology and card security:
I The contactless smart card contains an antenna embedded in the plastic body.
II The chip is powered on when brought into the reader's electromagnetic field.
III RBI set an upgrade target for ATMs by September 2017 to process EMV cards.
IV Despite EMV upgrades, ATM transactions based on magnetic stripes remain vulnerable to cloning.
V Contact chip processing of EMV cards ensures ATM infrastructure operates exclusively offline.

Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (IV) only
(B) (I), (II), (IV), and (V) only
(C) (II), (III), (IV), and (V) only
(D) All (I), (II), (III), (IV), and (V)

**May/June 2021**

**107.** Based on the case of Miss Verma shopping on an e-commerce website, answer the following question: The website prompts her to enter her credit card number, expiry date, and the 3-digit CVV number. In a separate dialog box, the site also asks her to input her secret 4-digit ATM PIN. Regarding the request for the ATM PIN alongside the CVV, what is the standard security protocol?
(A) One should never enter their PIN number when asked to provide the CVV online.
(B) The PIN is mandatory for all card-not-present online transactions.
(C) The PIN must be entered but mathematically added to the CVV for encryption.
(D) The PIN acts as a backup Token Reference Number in e-commerce.

**Oct/Nov 2021**

**108.** In the following questions, a statement of Assertion (A) is followed by a statement of Reason (R). Choose the correct option:
Assertion (A): Smart cards provide a higher level of security compared to magnetic stripe cards.
Reason (R): Smart cards perform complex decision-making tasks, including mutual authentication between the card and terminal.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).

Downloaded from www.pdf.tube

May/June 2007

**121.** Based on the case of "MegaMart" complying with the RBI mandate, answer the following question: To manage tokens effectively and handle potential fraud, what specific identifier has the RBI instructed merchants like MegaMart to create and store against each token?
(A) Token Vault ID
(B) Card Floor Limit
(C) Secure Electronic Signature
(D) Token reference number

Oct/Nov 2007

**122.** Based on the case of a startup "QuickBuy" integrating a payment gateway, answer the following question: Once a customer executes a purchase and the issuing bank verifies and approves the transaction, what is the next sequential action in the e-commerce processing cycle?
(A) The issuing bank generates a Charge Slip for the customer.
(B) The issuing bank physically dispatches a new token to the customer.
(C) The bank deposits funds into the merchant's account at a scheduled time.
(D) The payment gateway immediately revokes the merchant's Floor Limit.

May/June 2008

**123.** Based on the case of "MegaMart" complying with the RBI mandate, answer the following question: Under this framework, who holds the ultimate responsibility for the card tokenisation services rendered to MegaMart and its customers?
(A) The e-commerce merchant responsible for the checkout page.
(B) The individual consumers conducting the online transactions.
(C) The authorised card networks such as VISA, MasterCard, or RuPay.
(D) The Payment Gateway service provider hosting the connection.

Oct/Nov 2008

**124.** Based on the case of "MegaMart" complying with the RBI card tokenization mandate, answer the following question: Under this new system, if a customer uses the same single credit card to shop at MegaMart and two other separate online merchants, how are the tokens issued?
(A) Three different tokens will be issued, as tokens are unique for a combination of card and merchant.
(B) A single, universal token is issued for use across all three merchants.
(C) No tokens are issued; the customer must rely on a standard CVC2 code.
(D) A token is issued exclusively for the first merchant, leaving the other two to process via magstripe.

May/June 2009

**125.** Based on the case of "MegaMart" complying with the RBI mandate, answer the following question: For a customer who had previously allowed MegaMart to store their sensitive card details before the implementation of this mandate, what action is required?
(A) The stored details automatically convert into a lifetime valid physical card.
(B) The customer must register their card details afresh, while card networks issue tokens against them.
(C) MegaMart must retain the old data indefinitely alongside the new token.
(D) The customer must visit a bank branch to manually sign a token vault agreement.

NODIA

savings account.

**May/June 2024**

**115.** Based on the case of Mr. Sharma, an electronics showroom operator, answer the following question: The bank has assigned Mr. Sharma a specific transaction limit up to which he has discretion to accept cards without additional authorization. This limit is known as:
(A) The Card Limit
(B) The Hot Card Limit
(C) The Interchange Limit
(D) The Floor Limit

**Oct/Nov 2025**

**116.** Consider the following statements about POS terminals:
I A POS terminal reads information off a credit or debit card.
II It checks whether funds in the customer's bank account are sufficient.
III It transfers funds from the customer's account to the seller's account.
IV It records the transaction and strictly prints a receipt.
V POS systems are immune to employee theft, eliminating cashier collusion.
Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (V) only
(B) (I), (II), (III), and (IV) only
(C) (II), (III), (IV), and (V) only
(D) All (I), (II), (III), (IV), and (V)

**May/June 2005**

**117.** Based on the case of Miss Verma shopping online, answer the following question: If a website is a fraudulent platform designed to capture sensitive data, how does the website successfully bypass the security of the CVV?
(A) By utilizing an offline Floor Limit mechanism.
(B) By executing a Charge Back directly against the acquirer.
(C) By duplicating the track two data of the magnetic stripe remotely.
(D) By employing a Phishing scam tricking the cardholder into voluntarily entering the details.

**Oct/Nov 2005**

**118.** In the following questions, a statement of Assertion (A) is followed by a statement of Reason (R). Choose the correct option:
Assertion (A): The use of the CSC or CVV provides absolute, impenetrable protection against Phishing scams.
Reason (R): Phishers trick the cardholder into entering the CSC among other card details via fraudulent websites.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2006**

**119.** Based on the case of a university smart card system, answer the following question: When the balance on the university card is exhausted, students can approach a special terminal on campus, insert cash, and replenish the value on their card. Because the students can replenish the monetary value, these cards are specifically classified as:
(A) Reloadable cards
(B) Disposable cards
(C) EMV liability shift cards
(D) Contactless credit cards

**Oct/Nov 2006**

**120.** In the following questions, a statement of Assertion (A) is followed by a statement of Reason (R). Choose the correct option:
Assertion (A): EFTPOS is highly popular in Australia and New Zealand, capturing about 60% of retail transactions.
Reason (R): EFTPOS is an analog system that exclusively processes paper currency transfers at physical bank branches.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Click Here to Buy book on Amazon

(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2022**

**109.** Based on the case of a university smart card system used for the canteen and library, answer the following question: Students use these cards exclusively to purchase food in the canteen and pay for photocopying in the library. Based on the utility scope of the university's card, how is this payment ecosystem classified?
(A) An open loop debit card system.
(B) An international EFTPOS system.
(C) A dynamic token vault system.
(D) A closed stored value card system.

**Oct/Nov 2022**

**110.** In the following questions, a statement of Assertion (A) is followed by a statement of Reason (R). Choose the correct option:
Assertion (A): Card Tokenization aims to keep critical financial information secure from card data breaches.
Reason (R): Tokenization replaces actual card details with a unique alternate code preventing merchants from storing sensitive card numbers.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2023**

**111.** Based on the case of a startup "QuickBuy" integrating a payment gateway, answer the following question: The payment gateway integrated by QuickBuy employs cryptography to mask customer data, utilizing different keys for encryption and decryption. What is this method called?
(A) Symmetric cryptography
(B) Tokenization Reference cryptography
(C) Magnetic Track cryptography
(D) Asymmetric cryptography

**Oct/Nov 2023**

**112.** In the following questions, a statement of Assertion (A) is followed by a statement of Reason (R). Choose the correct option:
Assertion (A): The credit availed through a credit card gets renewed automatically upon repayment.
Reason (R): Bank credit cards are a type of consumer loan that is revolving in nature.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2025**

**113.** In the following questions, a statement of Assertion (A) is followed by a statement of Reason (R). Choose the correct option:
Assertion (A): The cost of domestic card transactions in India was historically high before the launch of RuPay.
Reason (R): There was a monopoly of foreign gateways like Visa and MasterCard in the Indian market.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

NODIA

**Oct/Nov 2024**

**114.** Based on the case of a university smart card system, answer the following question: In this university card system, when a student pays for a photocopy, how are the funds conceptually processed?
(A) They are routed through the Visa international network for verification.
(B) Funds are directly debited from the card itself and transferred to the vendor's terminal.
(C) They are delayed until the end of the billing cycle to generate a statement.
(D) They trigger a mandatory online authorization with the student's personal

# ANSWERS

1. (B) 4 digits
American Express cards utilize a four-digit numeric code for card verification, known as the CID. This specific security feature is typically printed on the front of the card, unlike other major brands that use three digits on the reverse. It serves to verify that the physical card is in the possession of the person making a remote transaction.

2. (C) By blocking credit card details from the merchant so only the involved bank can access the data.
The Secure Electronic Transaction protocol ensures high confidentiality by encrypting payment information so that only the financial institution can access sensitive details. This mechanism prevents merchants from seeing the cardholder's credit card information during a transaction. By isolating sensitive data, the protocol significantly reduces the risk of data theft or unauthorized use within the merchant's local environment.

3. (C) The commission earned by the acquirer and shared with the issuing bank.
Interchange refers to the commission earned by the acquiring bank during a credit card transaction. This fee is typically shared with the card-issuing bank to cover costs associated with transaction processing and risk management. It represents a vital component of the card business model, facilitating financial cooperation between various institutions involved in the processing cycle of consumer credit payments.

4. (C) Providing the CVV to an online merchant proves the user possesses the physical card and helps reduce fraud.
Providing a card verification value during an online transaction serves as proof that the user possesses the physical card. This security measure helps reduce fraudulent activities by ensuring that card details were not merely skimmed from a magnetic stripe. Unlike a personal identification number, it is used primarily for card-not-present transactions where the physical presence cannot be verified.

5. (B) Debit cards require a deposit balance, while credit cards utilize a bank-sanctioned credit limit.
Debit cards are linked to a personal deposit account where funds are deducted immediately upon purchase. In contrast, credit cards utilize a bank-sanctioned credit limit, allowing users to borrow funds up to a certain amount. This fundamental distinction centers on whether the transaction uses existing personal funds or a revolving line of credit provided by the issuing bank.

6. (B) Websites use SSL to authenticate identity, verified by the https prefix and a padlock symbol.
The Secure Socket Layer protocol is a standard cryptographic method used to establish an encrypted link between a web server and a browser. Websites use this protocol to authenticate their identity, which users can verify through the presence of an https prefix and a padlock symbol. It ensures that all data transmitted remains private and integral during online sessions.

7. (B) A revolving consumer loan that automatically renews within specific limits.
A bank credit card functions as a revolving consumer loan that automatically renews within specific limits once the cardholder repays the outstanding balance. It allows individuals to purchase goods and services without immediate payment. This financial tool provides a flexible line of credit, enabling consumers to manage their expenditures across different billing cycles based on their creditworthiness.

8. (B) CVC1 is for card-present magnetic stripe verification, while CVC2 is for card-not-present transactions.
Security codes for payment cards serve distinct purposes depending on the transaction environment. CVC1 is encoded within the magnetic stripe and is used for card-present transactions to verify the physical card's authenticity. Conversely, CVC2 is the printed

Downloaded from www.pdf.tube

**25.** (B) Cards are accepted universally across various issuers and merchants for general consumer purchases.
An open loop payment system is characterized by its universal acceptance across a wide range of merchants and financial institutions. Cards issued within such a system, like those on the RuPay or Visa networks, are not restricted to specific locations or closed environments. Instead, they can be used for general consumer purchases at any authorized terminal that supports the network's standards.

**26.** (D) An electronic device used to process card payments at retail locations through a combination of software and hardware.
A point of sale terminal is an electronic device designed to process card payments at retail locations. It utilizes a combination of hardware and software to read information from credit or debit cards, verify funds with the bank, and record transaction details. These terminals are essential for modern commerce, providing a secure and efficient way for businesses to accept electronic payments.

**27.** (A) The NPCI maintains ties with Discover Financial to enable international acceptance for RuPay cards.
To enable international acceptance for its domestic cards, the National Payments Corporation of India established a strategic partnership with Discover Financial Services. This agreement allows RuPay cardholders to use their cards at millions of merchant locations and automated teller machines outside of India. This expansion bridges the gap between the domestic scheme and global payment networks, facilitating easier international travel and commerce.

**28.** (A) New Zealand
Electronic funds transfer at point of sale systems are exceptionally popular in New Zealand, where they account for approximately sixty percent of all retail transactions. The widespread adoption of this technology has significantly reduced the reliance on cash for everyday purchases. Its efficiency and reliability have made it the preferred payment method for both consumers and merchants across the country's retail sector.

**29.** (C) The merchant submits a claim to the bank, which then pays the merchant for the goods or services.
In the standard application cycle of a credit card transaction, the merchant initiates the settlement process by submitting a claim to the bank. This claim represents the value of goods or services provided to the cardholder. The bank then verifies the transaction and pays the merchant for the purchase, effectively acting as an intermediary that provides immediate funding for the retail sale.

**30.** (D) It performs complex decision-making tasks, including mutual authentication to reduce fraud.
A primary conceptual advantage of smart cards is their ability to perform complex decision-making tasks directly on the card's internal chip. This includes executing mutual authentication protocols between the card and the terminal to verify legitimacy. By processing security checks internally rather than relying solely on external systems, smart cards provide much stronger protection against fraud and unauthorized access to sensitive data.

NODIA

**31.** (C) Asymmetric cryptography uses the exact same key for both encryption and decryption.
Asymmetric cryptography does not use the same key for both encryption and decryption; rather, it utilizes a pair of distinct but mathematically related keys. One key, known as the public key, is used to encrypt data, while a separate private key is required for decrypting it. This distinction is fundamental to maintaining secure communications over networks where a shared secret key is impractical.

**32.** (B) Individual e-commerce merchants (e.g., Zomato, Flipkart)
Under the card tokenization mandate, tokens are issued by authorized card networks such as Visa, MasterCard, and RuPay. Individual e-commerce merchants are not permitted to issue these tokens themselves. Instead, they must integrate with the card networks or payment gateways to request and store tokens on behalf of the customer, ensuring a standardized and secure process for replacing sensitive data.

efficiency and the potential risk of fraudulent card usage.

17. (A) Smart cards store more data than magnetic stripe cards and can perform calculations on that data.
Smart cards are equipped with embedded microprocessor chips that allow them to store significantly more data than traditional magnetic stripe cards. Beyond simple storage, these chips can perform complex calculations and execute security protocols like mutual authentication. This internal processing capability makes smart cards much more secure and versatile for various financial and non-financial applications compared to legacy stripe technology.

18. (C) 60%
According to data released by the Reserve Bank of India, the RuPay card network achieved a significant milestone in the domestic market. By the year 2020, it accounted for approximately sixty percent of the total card market share in India. This rapid growth highlights the success of the domestic payment scheme in competing with established international networks like Visa and MasterCard.

19. (D) It is a database storing the link between the sensitive card value and its corresponding token.
A token vault is a centralized, highly secure database that stores the relationship between sensitive card values and their corresponding encrypted tokens. When a transaction occurs, the vault allows the authorized system to map the token back to the original card details for processing. This architectural component ensures that sensitive information remains isolated and protected from potential exposure during digital transactions.

20. (A) It is powered on when brought into the electromagnetic field of the reader.
Contactless smart cards contain an embedded chip and an antenna that allow for seamless communication with a terminal. The internal chip draws its operational power through induction when the card is brought within the electromagnetic field generated by the reader. This eliminates the need for physical contact pins or an internal battery, enabling fast and convenient proximity-based transactions for users.

21. (C) NFC enables two nearby devices, such as a phone and terminal, to communicate with each other.
Near Field Communication is a short-range wireless technology that enables two nearby devices to establish communication. It is commonly used to facilitate transactions between a smartphone or a contactless card and a payment terminal. By operating over a very short distance, typically a few centimeters, it provides a secure and convenient method for transferring data and completing digital payments instantly.

22. (C) 3
During a standard credit card transaction at a retail location, a sale draft or charge slip is generated. Typically, three copies of this document are produced to ensure all parties have a record of the transaction. One copy is retained by the merchant, the second is given to the cardholder, and the third is sent to the bank for payment.

23. (C) The cardholder uses the sanctioned limit, which then automatically renews upon repayment of dues.
The revolving nature of a credit card refers to the way the sanctioned credit limit behaves over time. As the cardholder makes purchases, the available limit decreases. However, once the cardholder repays the outstanding dues, the credit limit is automatically restored to its original amount. This allows for continuous usage of the funds without the need for a new loan.

24. (D) Reloadable cards can have their value replenished by the consumer at a special terminal or ATM.
Reloadable smart cards offer a flexible payment solution where consumers can replenish the monetary value stored on the card. This can be done at specialized terminals or automated teller machines by paying cash or transferring funds. Unlike disposable cards, which must be discarded once the initial value is exhausted, reloadable cards allow for long-term use across multiple cycles of funding and spending.

Click Here to Buy book on Amazon

(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2014**

**96.** Based on the case of a startup "QuickBuy" integrating a payment gateway, answer the following question: Which of the following operates similarly to the secure channel integrated to route online transactions to a merchant account?
(A) Indicash
(B) CC Avenue
(C) India-1 ATM
(D) National Financial Switch

**May/June 2014**

**97.** Consider the following steps in an e-commerce transaction process:
I Customer purchases an item and enters card details.
II Payment gateway forwards information to the seller's bank.
III Seller's bank forwards information to the issuing bank.
IV Issuing bank verifies details and approves/denies the transaction.
V E-commerce service finally lets the buyer know if the transaction was approved or denied.
Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (IV) only
(B) (II), (III), (IV), and (V) only
(C) (I), (III), (IV), and (V) only
(D) All (I), (II), (III), (IV), and (V)

**Oct/Nov 2015**

**98.** Based on the case of Mr. Sharma, an electronics showroom operator using a POS terminal, answer the following question: In completing the sale draft for a television purchase using a credit card, Mr. Sharma retains one copy. Where are the other two copies directed according to standard procedures?
(A) One is given to the cardholder, and the second is sent to the bank for payment.
(B) Both copies are sent to the issuing bank for dual verification.
(C) One is sent to the local police station for anti-fraud tracking, and the other to the issuer.
(D) Both copies are securely archived at the POS terminal supplier's office.

**May/June 2017**

**99.** Based on the case of the university smart card system, answer the following question: If the university had chosen to issue cards that must be strictly discarded once the initial loaded value is exhausted without any option to replenish, those cards would be termed:
(A) Revolving credit cards
(B) Disposable cards
(C) White label cards
(D) Re-loadable cards

**Oct/Nov 2017**

**100.** In the following questions, a statement of Assertion (A) is followed by a statement of Reason (R). Choose the correct option:
Assertion (A): The RBI mandated an upgrade to process EMV chip and PIN cards at ATMs.
Reason (R): Transactions based on data from the magnetic stripe remain highly vulnerable to skimming and cloning.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2018**

**101.** Based on the case of a startup "QuickBuy" integrating a payment gateway, answer the following question: QuickBuy secures its website using a standard cryptographic protocol that places an 'https' prefix and a padlock symbol in the user's browser. This standard cryptographic protocol is:
(A) Secure Socket Layer (SSL)
(B) Near Field Communication (NFC)
(C) Electronic Funds Transfer at Point of Sale (EFTPOS)
(D) Contactless Smart Protocol

**Oct/Nov 2018**

**102.** Consider the following statements describing the tokenization mechanism:
I Tokenization uses a database called a token vault.
II The token vault stores the relationship between the sensitive value and the token.
III Tokenization reduces vulnerability to

NODIA

**33.** (B) Smart cards are highly vulnerable because their validation must always be conducted online.
Smart cards are designed with internal microprocessor chips that allow for high security and versatility. It is incorrect to claim they are highly vulnerable due to requiring only online validation. In fact, one of their key advantages is the ability to perform offline validation natively on the card. This feature enhances security and allows for transactions to proceed even without a constant network connection.

**34.** (D) It encrypts payment information so only the bank can see details, blocking the merchant.
The primary method used by the Secure Electronic Transaction protocol to protect consumer privacy is the encryption of payment information. This ensures that only the involved bank can access the sensitive card details, while the merchant is blocked from seeing them. By isolating the merchant from the actual credit card data, the protocol significantly reduces the likelihood of data theft at retail.

**35.** (A) It necessitates mandatory online validation for every single transaction due to lack of an internal chip.
It is incorrect to categorize the necessity of mandatory online validation as an advantage of a smart card. Smart cards are specifically designed with embedded chips that allow them to perform various functions, including the ability to conduct offline validation. This capability actually makes them more flexible and secure than magnetic stripe cards, which often rely on real-time external authorization for verification.

**36.** (A) The authorised card networks like VISA, MasterCard, and RuPay.
Following the directive from the Reserve Bank of India, the ultimate responsibility for providing and managing card tokenization services rests with authorized card networks. These networks, including Visa, MasterCard, and RuPay, are tasked with ensuring the security and integrity of the tokens generated. They oversee the technical infrastructure required to replace actual card details with unique identifiers across the digital ecosystem.

**37.** (A) The Floor Limit is an overall spending limit given to the cardholder, which is billed once a month.
The assertion that a floor limit is an overall spending limit given to the cardholder is incorrect. A floor limit actually refers to a per-transaction threshold fixed by the acquiring bank. Transactions below this amount can be accepted by merchants at their discretion without needing prior authorization. The overall maximum amount a cardholder can spend is instead defined by the card limit.

**38.** (D) Discover Financial
While CC Avenue, PayUMoney, and BillDesk are well-known payment gateways operating within the Indian market, Discover Financial Services is categorized as an international card network. It provides the infrastructure for card acceptance globally and has partnerships for domestic schemes like RuPay, but it does not function primarily as a payment gateway for e-commerce merchants in the same capacity.

**39.** (D) Cards issued by separate banks that are mutually acceptable across over 1500 different merchants.
In an open system, an electronic purse or wallet is characterized by its mutual acceptance across a diverse group of merchants and issuers. A prime example occurred during the 1996 Olympics, where cards issued by various banks were accepted by over fifteen hundred different vendors. This contrasts with closed systems, which restrict the card's use to specific locations or narrow services.

**40.** (D) Despite advanced POS technology, systems remain invulnerable to dishonest cashiers entering lower quantities to profit.
Claiming that point of sale systems are entirely invulnerable to dishonest practices is incorrect. Despite advanced technology, these systems can still be susceptible to human manipulation, such as cashiers entering lower quantities to profit. While automation significantly reduces errors and fraud, it does not completely eliminate the possibility of collusion or internal theft within a retail environment where hardware is managed manually.

NODIA

**41.** (B) (II), (IV), (I), (III)
A credit card transaction follows a specific chronological sequence starting with the cardholder making a purchase from a merchant. Next, the merchant submits a claim to the bank, and the bank pays the merchant for the purchase. Subsequently, the bank sends a notice to the customer to make payment. Finally, the cardholder completes the cycle by paying the bank.

**42.** (C) CVV provides absolute protection against scammers who have already acquired the card number.
The statement that the card verification value provides absolute protection against scammers who already have the card number is incorrect. While it is a significant security feature, it cannot prevent fraud if the code itself is compromised through methods like phishing. In such cases, scammers trick users into revealing the code, thereby bypassing the protection intended by the physical card requirement.

**43.** (B) A single unique token is universally issued per card to be utilized across all merchants.
Within the card tokenization framework, a single universal token is not issued for use across all merchants. Instead, tokens are unique for a specific combination of the card, the token requestor, and the device used. This means that if a consumer uses the same card at different online stores, each store will have a distinct token associated with that card.

**44.** (D) DFS
Companies like TSMC, NXP, and Global Foundries are recognized for their roles in the semiconductor industry and the manufacturing of integrated circuits used in smart cards. Conversely, Discover Financial Services is an international payment network and card issuer. It provides the financial infrastructure for transactions but is not involved in the physical manufacturing of the silicon chips for cards.

**45.** (C) Near Field Communication (NFC)
For mobile payment solutions like Apple Pay and Android Pay to achieve universal adoption, devices must be equipped with Near Field Communication technology. This short-range wireless standard allows smartphones to communicate securely with payment terminals by simply being held near the reader. It is the fundamental technical requirement that enables the seamless exchange of encrypted payment tokens at the point of sale.

**46.** (B) A credit card holder must maintain a savings account and balance with the issuing bank.
It is incorrect to state that a credit card holder must maintain a savings account and balance with the issuing bank. Unlike a debit card, which requires a direct link to an existing personal deposit account for immediate fund withdrawal, a credit card provides access to a pre-approved line of credit. Payments for credit card dues can be made from any bank account.

**47.** (B) Phishing scams that trick the cardholder into entering the CSC on a fake website.
The real-world effectiveness of the card verification value as an anti-fraud device is most severely diminished by phishing scams. These malicious attacks trick cardholders into voluntarily entering their security code on fraudulent websites. Once the scammer obtains the code along with other card details, the security intended by requiring physical possession of the card is completely bypassed, leading to unauthorized transactions.

**48.** (B) The prospect of a truly cashless society was fully realized by the deployment of the first-generation ATMs alone.
The idea that the prospect of a truly cashless society was fully realized solely by the deployment of first-generation automated teller machines is incorrect. While ATMs revolutionized access to cash and banking services, they did not eliminate the need for physical currency. A cashless society requires a broader digital payment ecosystem, including point of sale technology, online banking, and mobile payment platforms.

**49.** (A) International transactions processed across foreign e-commerce portals.
The mandatory card tokenization framework directed by the Reserve Bank of India specifically focuses on securing domestic e-commerce transactions within the country. It does not currently cover international transactions processed across foreign portals. Therefore, while domestic purchases must follow the new security

Downloaded from www.pdf.tube

rules for storing card details, international transactions remain exempt from this particular mandate for the time being.

**50.** (C) CoFT
CVC1, CVC2, and iCVV are all recognized types of security codes used to verify the authenticity of payment cards during various transaction scenarios. In contrast, CoFT stands for Card on File Tokenization. It refers to a framework and a process for securing card data through tokenization rather than representing a specific numeric security code printed or encoded on the physical card.

**51.** (D) A token is unique for a combination of the card, token requestor, and the device used.
The uniqueness of a token under the Card on File Tokenization framework is defined by a specific combination of three factors. A token is generated uniquely for the specific card, the token requestor such as an e-commerce platform, and the physical device being used for the transaction. This multi-layered uniqueness ensures that a compromised token cannot be easily reused in different contexts.

**52.** (D) NPCI has completely avoided integrating EMV chip technology to ensure RuPay cards remain uniquely signature-based.
It is incorrect to claim that the National Payments Corporation of India avoided integrating EMV chip technology for RuPay cards. In reality, NPCI rolled out chip-based cards that feature embedded microprocessors to enhance security for PIN-based transactions. These modern cards comply with international security standards, moving away from older signature-based magnetic stripe technology to better protect consumers from skimming and fraud.

**53.** (C) The merchant directly demands monthly interest payments from the cardholder for the sold goods.
In a standard credit card transaction cycle, the merchant does not directly demand interest payments from the cardholder for the goods sold. Instead, the merchant receives payment from the bank after submitting a claim. Any interest or finance charges are managed between the issuing bank and the cardholder, depending on whether the balance is paid in full within the billing cycle.

**54.** (C) They remain highly susceptible to skimming and cloning frauds.
The most critical vulnerability affecting transactions that rely on magnetic stripes is their high susceptibility to skimming and cloning. Because the data on a magnetic stripe is static and can be easily copied by fraudulent devices, criminals can create duplicate cards to perform unauthorized transactions. This weakness led to the mandatory upgrade to EMV chip technology, which provides much stronger data protection.

**55.** (A) Issues and manages a dynamic token vault for all retail merchant accounts.
Issuing and managing a dynamic token vault for merchant accounts is not a function performed by a point of sale terminal. Instead, this task is handled by centralized databases managed by card networks or financial institutions. The POS terminal itself focuses on reading card data, verifying funds, and recording specific transaction details to facilitate the immediate transfer of funds for retail purchases.

**56.** (A) Phone cards and subway cards are primary examples of open system stored value cards.
Claiming that phone cards and subway cards are primary examples of open system stored value cards is incorrect. These cards are actually characteristic of closed systems, as they are restricted to specific locations or narrow services provided by a single issuer. In contrast, an open system involves cards issued by various banks that are mutually acceptable across many different merchants.

**57.** (A) By networking institutions into a system linking people far beyond physical buildings.
Automated teller machines began to blur the divisions between banks by networking multiple institutions into a cohesive system. This connectivity allowed people to access financial services far beyond the physical boundaries of a specific bank branch. By enabling transactions across different networks and locations, ATMs transformed individual banks into part of a broader, interconnected financial infrastructure that operates around the clock.

NODIA

cardholder and the funds are reclaimed by the bank.

**77.** (D) (I), (II), and (III)
All three statements accurately describe the functions of a payment gateway. It provides a secure connection between an e-commerce entity and a merchant account, verifies transactions in real time, and utilizes data encryption algorithms to protect information from unauthorized access. These features are essential for ensuring the integrity and security of financial transactions conducted over the internet for various online businesses.

**78.** (A) P-2, Q-1, R-4, S-3
A point of sale terminal is a retail device used to check funds and transfer money. Near Field Communication is a contactless technology for close-range device communication. The National Common Mobility Card is a contactless smart card used for transit systems. Finally, EFTPOS is an electronic payment system that is highly popular in countries like Australia and New Zealand.

**79.** (D) Both (I) and (II) are incorrect.
Both statements regarding the consumer aspect of tokenization are incorrect. Cardholders are not required to pay a mandatory fee to banks for the generation of tokens for online domestic transactions. Furthermore, tokenization does not apply strictly to international transactions; in fact, the current mandate in India specifically targets and covers domestic purchases to enhance the security of the local digital ecosystem.

**80.** (D) Storage capability - Merchants allowed to store Card CVV post-July 2022.
The assertion that merchants are allowed to store the card verification value after July 2022 is incorrect. The Reserve Bank of India's mandate specifically prohibits merchants from storing sensitive card details, including the CVV, to enhance security. Under the new rules, only authorized card networks and issuers can maintain such information, while merchants must rely on tokens for processing recurring transactions.

**81.** (A) (I), (II), and (III)
The Secure Electronic Transaction protocol was developed by Visa and MasterCard to ensure confidentiality and authenticity through digital signatures. It successfully prevents merchants from accessing sensitive card details by encrypting the information for the bank's eyes only. However, the claim that it mandates the installation of customized biometric hardware by all merchants is incorrect, as the protocol focuses on software-based security.

**82.** (A) P-2, Q-4, R-3, S-1
A payment gateway provides a secure connection for online transaction processing. Data encryption uses cryptographic keys to mask information during transmission. Secure Socket Layer is a standard protocol for establishing encrypted links between web servers and browsers. Finally, the Secure Electronic Transaction protocol utilizes digital signatures to block merchants from seeing sensitive credit card details, ensuring high levels of privacy.

**83.** (A) P-4, Q-1, R-2, S-3
In 1996, open system Visa cards were widely used during the Olympics. By 2015, mobile payment solutions like Android Pay and Apple Pay were launched. The Motioncode technology for dynamic CVVs was introduced in 2016. Finally, in 2022, the Reserve Bank of India mandated the implementation of card tokenization for online transactions to improve the security of the digital payment landscape.

**84.** (A) (I) and (II) only
RuPay chip cards utilize embedded microprocessors for secure PIN-based transactions, and the network maintains an agreement with Discover Financial Services for international acceptance. However, the statement that National Common Mobility Cards are exclusively restricted to Metro train services is incorrect. These cards are designed for a wider range of transit and retail uses across different transport systems and participating merchant locations.

**85.** (D) Both (I) and (II) are incorrect.
Both statements regarding card technologies are incorrect. A conventional magnetic stripe typically stores information across three tracks,

Click Here to Buy book on Amazon

**67.** (A) (II), (IV), (I), (III)
The e-commerce transaction process begins when a customer enters card details to purchase an item. The payment gateway then forwards this information to the seller's bank. Subsequently, the seller's bank communicates with the card-issuing bank for authorization. Finally, the issuer verifies the details, approves the transaction, and sends the confirmation back to the seller's bank to complete the sale.

**68.** (C) Both (I) and (II) are correct.
Both statements are correct regarding the operations of credit cards. If a cardholder defaults on payments or exceeds their spending limit, the issuer may place the card on a hot list to prevent further use. Additionally, credit cards inherently offer a revolving line of credit that automatically renews as the outstanding balance is repaid by the user over different billing cycles.

**69.** (D) (I), (II), and (III)
Stored value cards, also known as prepaid cards, function by having the consumer pay a bank for a card pre-loaded with a specific monetary value. When used, funds are directly debited from the card itself and transferred to the vendor's terminal. This process does not require a formal bank account for the transaction, making these cards a convenient payment tool.

**70.** (A) P-3, Q-4, R-2, S-1
A token vault is a database storing the link between sensitive card values and tokens. Card on File Tokenization refers to the replacement of actual card details with alternate codes. Token reference numbers are identifiers created and stored by merchants for each token. Finally, authorized card networks are the entities ultimately responsible for providing the tokenization services to the financial ecosystem.

**71.** (B) (I), (II), and (III)
Under the tokenization mandate, consumers generally will not view or know their specific token details, which are generated as distinct sixteen-digit numbers. Banks are also required to provide portals for cardholders to manage or delete these tokens. However, the claim that consumers must pay a mandatory fee for token generation is incorrect, as this service is typically provided without additional charge.

**72.** (A) P-4, Q-2, R-1, S-3
Visa and MasterCard typically fix the issuer's portion of the commission, while American Express uses a four-digit numeric code for its card verification. The National Payments Corporation of India is the creator of the RuPay domestic card scheme. Lastly, the Reserve Bank of India is the regulatory body that mandated card tokenization to secure online transactions within the country.

**73.** (A) Only (I) is correct.
It is correct that the Reserve Bank of India set a target for banks to upgrade ATMs by September 2017 to process EMV chip and PIN cards. However, the claim that the NPCI continues to route all magnetic stripe transactions to encourage legacy infrastructure is false. On the contrary, the shift towards EMV technology is specifically intended to phase out insecure stripe-based transactions.

**74.** (C) Closed System Card - Usable only in specified locations like mass-transit.
A closed system card is correctly defined as a payment card that can only be used in specified locations, such as a mass-transit system or a university campus. In contrast, magnetic stripes do not contain microprocessors, and stored value cards do not require a mandatory checking account. These definitions help distinguish between localized payment ecosystems and broader, open financial networks.

**75.** (B) (I), (II), and (III)
Smart cards offer high data security and the ability to perform complex tasks like mutual authentication and offline validation. These features make them significantly more robust than traditional magnetic stripe cards. However, the claim that they strictly require the user to possess a regular bank deposit account is incorrect, as stored value smart cards can be used by individuals without a bank account.

**76.** (A) P-2, Q-4, R-1, S-3
An acquirer is the bank that has an agreement with the merchant, while an issuer is the bank that sends transaction statements to the cardholder. Interchange refers to the commission earned by the acquiring bank during processing. A chargeback describes a situation where an authorized transaction is later disputed by the

NODIA

**58.** (A) Users are completely exempt from requesting a new token even if a fraud is detected against an active token.
The statement that users are exempt from requesting a new token if fraud is detected against an active one is incorrect. In such circumstances, a new token must be generated to maintain the security of the account. The tokenization mandate ensures that compromised identifiers can be easily revoked and replaced, protecting the underlying card details from further risk without requiring a new card.

**59.** (C) The ability to buy goods and services without paying for them immediately.
The primary utility of a credit card for a consumer is the ability to purchase goods and services without the need for immediate payment. It provides a revolving line of credit that allows users to manage their cash flow by deferring the settlement of their expenditures. This financial flexibility is a key advantage, enabling consumers to make necessary purchases across different billing cycles.

**60.** (B) Entering the CVV number directly into an ATM to authorize a cash advance.
One should never enter their secret personal identification number when an online merchant requests the card verification value. The CVV is intended for card-not-present transactions to verify physical possession of the card, while the PIN is generally reserved for card-present or ATM transactions. Confusing the two or providing both can compromise the security of the cardholder's financial account.

**61.** (A) P-3, Q-4, R-2, S-1
CC Avenue is a well-known payment gateway, while TSMC is a major manufacturer of smart card chips. Discover Financial Services acts as an international network that maintains ties with RuPay for global acceptance. Finally, Indicash is a provider of white label automated teller machines in India. These pairings correctly identify the specific industry roles and categories for each organization listed.

**62.** (A) Only (I) is correct.
It is correct that Secure Socket Layer uses a padlock symbol and the https prefix to authenticate website identity for users. However, the claim that Transport Layer Security is outdated and was replaced by SSL is incorrect. In reality, TLS is the more modern and secure successor that has replaced SSL in standard cryptographic protocols for securing communications over computer networks.

**63.** (B) P-4, Q-1, R-3, S-2
Credit cards provide a revolving loan up to a limit, whereas debit cards trigger immediate payments from a deposit account. Smart cards are distinguished by an embedded computer chip for data storage and calculations. Closed stored value cards are restricted for use in specific locations like mass-transit systems. These characteristics accurately define the fundamental differences between these various payment card types.

**64.** (D) (I), (II), and (III)
All three statements accurately reflect the rules of the card tokenization mandate. Merchants are required to delete previously stored sensitive card information to improve security. A single card will indeed generate distinct tokens for different merchants to ensure compartmentalization. Furthermore, consumers retain the option to manually enter their details for one-time purchases if they choose not to save their card information.

**65.** (A) VISA - 3 digit numeric code
Visa cards utilize a three-digit numeric code for card verification, which is typically found on the signature panel on the reverse of the card. This is also standard for MasterCard and Discover cards. In contrast, American Express uses a four-digit code printed on the front. These security codes are essential for verifying the physical presence of the card during online transactions.

**66.** (A) (I), (II), and (IV)
It is true that CVC1 is retrieved during card-present transactions and CVC2 is used for card-not-present scenarios. The Motioncode system also successfully addresses the static nature of these codes by refreshing them periodically. However, the claim that these codes offer robust, unbreakable protection against phishing is false, as scammers often trick users into voluntarily revealing their sensitive security details.

Downloaded from www.pdf.tube

not four. Additionally, smart cards actually possess a much higher data storage capacity compared to legacy magnetic stripe cards, thanks to their embedded microprocessor chips. These chips allow for the storage of complex data and the execution of sophisticated security protocols during transaction processing.

**86.** (A) P-3, Q-4, R-1, S-2
CVC1 is encoded on track two for card-present transactions, while CVC2 is sought by merchants for card-not-present internet transactions. The iCVV is an electronic code supplied by contactless and chip cards for verification. Finally, Motioncode represents a dynamic code that automatically refreshes every hour. These codes are essential for maintaining security across various types of modern electronic payment environments.

**87.** (A) (I), (II), and (IV)
Credit card users access a line of credit, and debit card users must maintain a bank balance for immediate payments. It is also true that credit card repayments can be made from any other bank account. However, the claim that credit card payments are immediate by debiting the holder's account is false, as these transactions are billed periodically.

**88.** (A) P-2, Q-1, R-3, S-4
A floor limit is a discretionary per-transaction amount fixed by the acquirer. The card limit is the maximum spending amount restored upon payment. The hot list is a database used to track lost, stolen, or defaulting cards for retrieval. Finally, the billing cycle is the periodical interval at which the issuer sends a transaction statement to the cardholder.

**89.** (A) (I) and (II) only
Cardholders are generally given two weeks to pay their billed amount, and the acquirer pays the merchant the sale draft amount minus a commission. However, the claim that the commission earned by the acquirer is never shared with the issuing bank is incorrect. In practice, a portion of this commission, known as interchange, is shared with the issuer.

**90.** (A) Payment Gateway - NXP
CC Avenue, Instamojo, and BillDesk are all prominent payment gateways operating in the Indian market. In contrast, NXP is a major semiconductor company that manufactures the chips used in smart cards and other electronic devices. It provides the hardware components for the payment ecosystem but does not function as a payment gateway service that routes transactions for e-commerce entities.

NODIA

**91.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Both the assertion and the reason are true, and the reason correctly explains the assertion. A debit card requires the customer to maintain a bank account and an available balance because the technology is designed to trigger immediate payments. This occurs by directly debiting the holder's personal deposit account for the transaction amount at the exact time of the purchase.

**92.** (C) Charge Back
When a transaction is disputed by a cardholder and the issuing bank reclaims the funds from the acquirer after verifying the dispute, the process is known as a chargeback. This mechanism protects consumers from unauthorized charges or unsatisfactory service. It serves as a critical safety feature in the credit card industry, shifting financial responsibility back to the merchant.

**93.** (A) (I), (II), (III), and (IV) only
Statements regarding CVC1 being on track two for card-present transactions and the limitations of static codes are correct. The usage of CVC2 for internet transactions is also accurately described. However, the claim that iCVV or dynamic codes are supplied strictly by magnetic stripes is false, as these are electronically generated by the chips in smart cards or contactless devices.

**94.** (C) CVC2
The three-digit security code found on the reverse of a payment card, which merchants often request for internet transactions, is technically known as CVC2. This code is used specifically for card-not-present scenarios to verify that the person initiating the purchase has physical possession of

**113.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Both the assertion and the reason are true, and the reason correctly explains the assertion. Historically, the cost of domestic card transactions in India was high due to the monopoly of foreign card networks like Visa and MasterCard. These international gateways charged significant fees for their services, leading to the development and launch of RuPay as a cost-effective domestic alternative.

**114.** (B) Funds are directly debited from the card itself and transferred to the vendor's terminal.
In a closed system like the university smart card system, the monetary value is stored directly on the card itself. When a student makes a purchase, the funds are conceptually processed by being immediately debited from the card and transferred to the vendor's terminal. This localized transaction does not require a formal bank account or real-time external network authorization.

**115.** (D) The Floor Limit
The specific transaction limit up to which a merchant can accept card payments without seeking additional authorization from the issuer is known as the floor limit. This amount is fixed by the acquiring bank to facilitate faster retail processing for smaller purchases. It gives the merchant a degree of discretion while balancing the risk of potential fraudulent activity for larger transactions.

**116.** (B) (I), (II), (III), and (IV) only
Point of sale terminals read card information, check for sufficient funds in the customer's account, and facilitate the transfer of money to the seller. They also record the transaction and print a receipt. However, the claim that these systems are entirely immune to employee theft is false, as they can still be vulnerable to manipulation or collusion in retail environments.

**117.** (D) By employing a Phishing scam tricking the cardholder into voluntarily entering the details.
Fraudulent websites successfully bypass the security of the card verification value by using phishing scams. These malicious platforms trick the cardholder into voluntarily entering their sensitive details, including the CVV, by appearing as a legitimate store. Once the user provides this information, the scammer can use it to perform unauthorized transactions, effectively circumventing the protection intended by the code.

**118.** (D) Assertion (A) is false, but Reason (R) is true.
The assertion that the card verification value provides absolute, impenetrable protection against phishing scams is false. However, the reason provided is true, as phishers do indeed trick cardholders into entering the code via fraudulent websites. Because the code can be compromised through such social engineering tactics, it does not offer the absolute security that the assertion incorrectly suggests it provides.

**119.** (A) Reloadable cards
Cards that allow users to replenish the stored monetary value after it has been exhausted are specifically classified as reloadable cards. Users can add funds to these cards at specialized terminals or ATMs, enabling long-term and repeated use. This distinguishes them from disposable cards, which are meant to be used once and then discarded after the initial balance is spent.

**120.** (C) Assertion (A) is true, but Reason (R) is false.
The assertion that EFTPOS is highly popular in Australia and New Zealand is true. However, the reason is false because EFTPOS is actually an electronic payment system that processes digital funds transfers at retail locations using cards, rather than an analog system that deals with paper currency at bank branches. Therefore, the reason incorrectly describes the nature of this technology.

**121.** (D) Token reference number
To effectively manage tokens and address potential issues like fraud, the Reserve Bank of India has instructed merchants to create and store a specific identifier against each token. This identifier is known as the token reference number. It allows the merchant to track the transaction without needing to store the sensitive card details or the actual token used in the purchase.

Click Here to Buy book on Amazon

**104.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Both the assertion and the reason are true, and the reason correctly explains the assertion. The Secure Electronic Transaction protocol is specifically designed to block merchants from seeing sensitive credit card details. It achieves this by encrypting the payment information in a way that only the involved bank can access and view the data, thereby ensuring high levels of privacy.

**105.** (C) Motioncode (Dynamic CVV)
Motioncode is a security technology that replaces the static three-digit code on the back of a payment card with a dynamic one that refreshes automatically, usually every hour. This innovation ensures that even if card details are captured by an unauthorized party, the security code will soon become invalid. It provides a robust defense against various types of online fraud.

**106.** (A) (I), (II), (III), and (IV) only
It is correct that contactless cards use embedded antennas and are powered by the reader's electromagnetic field. The RBI also set upgrade targets for EMV processing to combat the vulnerability of magnetic stripes. However, the claim that contact chip processing ensures the infrastructure operates exclusively offline is false, as most EMV transactions still require online connectivity for real-time authorization.

**107.** (A) One should never enter their PIN number when asked to provide the CVV online.
According to standard security protocols, a cardholder should never enter their secret personal identification number when asked to provide a card verification value online. The PIN is intended for secure authentication at physical terminals or ATMs, while the CVV is for card-not-present transactions. Legitimate e-commerce websites will not ask for an ATM PIN as part of the checkout process.

**108.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Both the assertion and the reason are true, and the reason correctly explains the assertion. Smart cards provide superior security compared to magnetic stripe cards because they are capable of performing complex decision-making tasks. This includes executing mutual authentication between the card and the terminal, which ensures that both the card and the reader are legitimate before a transaction proceeds.

**109.** (D) A closed stored value card system.
The payment ecosystem described, where cards are used exclusively for specific services within a university like the canteen and library, is classified as a closed stored value card system. These cards are restricted to a defined environment and cannot be used for general purchases at external merchants. This distinguishes them from open systems that enjoy universal acceptance across networks.

**110.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Both the assertion and the reason are true, and the reason correctly explains the assertion. Card tokenization is designed to secure critical financial data from breaches by replacing actual card details with a unique alternate code. This prevents merchants from storing sensitive card numbers, thereby ensuring that even if a merchant's database is compromised, the actual card information remains protected.

**111.** (D) Asymmetric cryptography
The method of employing different keys for encryption and decryption to securely mask data is known as asymmetric cryptography. This approach uses a public key to encrypt information and a separate, private key to decrypt it. It is a fundamental security technique used by payment gateways to ensure that sensitive customer data is protected from unauthorized access during network transmission.

**112.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Both the assertion and the reason are true, and the reason correctly explains the assertion. The credit availed through a credit card is renewed automatically upon repayment because these cards are a type of revolving consumer loan. This structure allows users to continuously spend up to their sanctioned limit as long as they pay back the outstanding balance over time.

Downloaded from www.pdf.tube

the card. It acts as an additional layer of security beyond the standard card number.

**95.** (C) Assertion (A) is true, but Reason (R) is false.
The assertion that data encryption uses algorithms to securely transmit data is true. However, the reason provided is false because symmetric cryptography actually uses the same identical key for both encryption and decryption. Using different keys for these processes is instead a characteristic of asymmetric cryptography. Therefore, the reason does not correctly describe the symmetric method of data masking.

**96.** (B) CC Avenue
CC Avenue is a prominent example of a payment gateway that provides a secure channel for routing online transactions to merchant accounts. It functions as an intermediary between the e-commerce website and the banking networks, ensuring that payment data is encrypted and processed safely. This service is essential for startups and established businesses looking to accept digital payments from customers.

**97.** (D) All (I), (II), (III), (IV), and (V)
All the listed steps accurately describe the chronological cycle of an e-commerce transaction. The process begins with the customer entering details, followed by the payment gateway forwarding information to the banks for verification and approval. Finally, the system informs the buyer of the outcome. This comprehensive sequence ensures that every digital purchase is securely authorized and processed through the financial ecosystem.

**98.** (A) One is given to the cardholder, and the second is sent to the bank for payment.
In a standard credit card transaction, the generated sale draft typically has three copies to ensure all parties have a record. The merchant retains one copy for their own business records. Of the remaining two copies, one is provided to the cardholder as a receipt, and the other is sent to the bank to facilitate the settlement process.

**99.** (B) Disposable cards
Cards that are issued with a pre-loaded monetary value and must be discarded once that value is exhausted are known as disposable cards. These cards do not offer the option for the user to replenish or reload funds after the initial amount is spent. This distinguishes them from reloadable cards, which allow for continuous use through multiple cycles of funding.

**100.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Both the assertion and the reason are true, and the reason correctly explains the assertion. The Reserve Bank of India mandated the upgrade to EMV chip and PIN technology because traditional magnetic stripe transactions are highly vulnerable to skimming and cloning. By shifting to more secure chip-based processing, the banking system aims to significantly reduce fraud and protect consumer data.

**101.** (A) Secure Socket Layer (SSL)
The standard cryptographic protocol that uses an https prefix and a padlock symbol to secure websites is known as Secure Socket Layer. It creates an encrypted link between a web server and a browser, ensuring that all data passed between them remains private. This authentication is vital for online businesses to build trust with customers and protect sensitive payment information.

**102.** (C) (I), (II), (III), and (V) only
Tokenization utilizes a secure database called a token vault to store the relationship between tokens and sensitive card values, effectively reducing fraud. Major payment platforms like Apple Pay also operate on this system. However, the claim that the token concept was entirely new to India in 2022 is false, as tokenization technologies have been present in various forms before that.

**103.** (B) Interchange
The commission earned by an acquiring bank when it processes sales drafts for a merchant is known as interchange. This fee typically ranges from 2% to 3.5% of the transaction value and is used to cover the costs of processing and managing financial risks. A portion of this fee is shared with the bank that issued the payment card.

NODIA

**122.** (C) The bank deposits funds into the merchant's account at a scheduled time.
Once the issuing bank verifies and approves a transaction in the e-commerce processing cycle, the next sequential action involves the settlement of funds. The bank will schedule a transfer to deposit the payment into the merchant's account. This step ensures that the seller receives the money for the goods or services provided to the cardholder during the online checkout.

**123.** (C) The authorised card networks such as VISA, MasterCard, or RuPay.
Under the Reserve Bank of India's mandate, the ultimate responsibility for the card tokenization services provided to merchants and customers rests with the authorized card networks. These networks, such as Visa, MasterCard, and RuPay, are responsible for the technical infrastructure and the security of the tokens generated, ensuring that sensitive card data is correctly replaced and managed across the ecosystem.

**124.** (A) Three different tokens will be issued, as tokens are unique for a combination of card and merchant.
Under the tokenization framework, tokens are unique for a specific combination of card and merchant. Therefore, if a customer uses the same credit card at three separate online merchants, three different and distinct tokens will be issued. This compartmentalization ensures that a security breach at one merchant does not compromise the tokenized data stored with the other participating online stores.

**125.** (B) The customer must register their card details afresh, while card networks issue tokens against them.
For customers who had previously allowed merchants to store their sensitive card details, the implementation of the mandate requires a fresh action. The customer must register their card details again with the merchant, at which point the authorized card networks will generate and issue tokens against them. This process ensures that old, insecurely stored data is replaced by secure tokenized identifiers.

www.nodia.in

Click Here to Buy book on Amazon

Oct/Nov 2008

**32.** Which of the following is NOT an on-line bill presentment and payment model?
(A) Biller direct model
(B) Acquirer-centric model
(C) Consolidator model
(D) Hybrid model

May/June 2006

**33.** Which of the following is incorrectly categorized as a feature of Contracts as digital objects?
(A) They can include instructions regarding handling, routing, storing, and scheduling.
(B) They inherently include the user profile's personal secrets and likes/dislikes.
(C) They can be negotiated, including prices, terms of payment, and penalties.
(D) In many instances, they can be bought, sold, and exchanged.

Oct/Nov 2017

**34.** What best describes the dual benefit of personalization in Electronic Bill Presentment and Payment (EBPP)?
(A) It reduces paper usage and eliminates the need for internet access.
(B) It allows the consolidator to manage the billing process while deleting bill details entirely.
(C) It increases the pre-delivery float time while decreasing the transaction speed.
(D) It helps deliver the right products leading to repeat sales, and promotes the perception of a one-to-one personal relationship.

May/June 2008

**35.** Which of the following is NOT mentioned as a standard for e-business?
(A) TDM (Time Division Multiplexing)
(B) OBI (Open Buying on Internet)
(C) JEPI (Joint Electronic Payment Initiative)
(D) OFX (Open Financial Exchange)

Oct/Nov 2013

**36.** Which represents the best definition of the "open-loop" characteristic in Real-Time Payments?
(A) Payments are directly connected to personal accounts instead of relying on a prepaid balance to accelerate the process.
(B) Payments are processed exclusively through a third-party prepaid aggregator.
(C) Payments cycle continuously without final settlement in the merchant's account.
(D) Payments require the sender and receiver to use the exact same mobile application.

May/June 2015

**37.** Which of the following is incorrectly stated as a benefit of Supply Chain Management (SCM)?
(A) Increase in order entry errors leading to extensive manual rework.
(B) Lower operating costs through reduced inventory.
(C) Improve productivity through better data integrity.
(D) Faster communications and an improved competitive position.

Oct/Nov 2012

**38.** Which of the following is NOT a categorization of payments based on value?
(A) Micro-Payments
(B) Mini-Payments
(C) Macro-Payments
(D) Mega-Payments

May/June 2011

**39.** What is the best description of Voice Biometrics in call center technologies?
(A) An automated phone system that routes calls based on keypad inputs.
(B) A software application used to forecast the volume of customer interactions.
(C) A telephony system that recognizes and routes incoming calls to the best suited terminal.
(D) A reliable method to authenticate a person's identity based on unique vocal characteristics to prevent fraud.

Oct/Nov 2020

**40.** Which statement is incorrectly attributed to Buy Now, Pay Later (BNPL) trends?
(A) It allows customers to spread payments over a set period of time.
(B) Many consumer BNPL products provide credit decisions in minutes.
(C) BNPL products are generally easier to obtain than traditional credit cards.
(D) Customers must pay substantial interest charges on every installment regardless of the provider.

NODIA

Oct/Nov 2014

**8.** What characterizes a pull message in SMS banking?
(A) It is generated automatically by the bank for a large withdrawal.
(B) It is initiated by the customer using a mobile phone for obtaining information or performing a transaction.
(C) It is exclusively used for marketing messages sent by the financial institution.
(D) It is a one-time password required to complete online transactions.

May/June 2019

**9.** Which statement accurately describes the Private label online business model?
(A) The e-commerce player owns the inventory and manages the supply chain directly.
(B) An e-commerce company sells its own brand goods through its website, typically earning higher margins.
(C) Sellers partner with leading marketplaces to set up a dedicated online store on the latter's website.
(D) A branded online store is managed by a third party taking responsibility for website traffic.

Oct/Nov 2006

**10.** Which entity functions as the authorized Bharat Bill Payment Central Unit (BBPCU)?
(A) RBI
(B) SBI
(C) NPCI
(D) IDRBT

May/June 2021

**11.** Which statement reflects current trends in cybersecurity for payments?
(A) The industry is reducing investments in behavioral biometrics to favor passwords.
(B) Cyber threats have decreased due to the rise of non-cash payments.
(C) AI-based authentication prompts are being phased out in favor of manual verification.
(D) Security and online privacy emerged as the top two priorities for e-commerce customers, ahead of convenience.

Oct/Nov 2010

**12.** What defines a digital object in electronic commerce building blocks?
(A) A physical server utilized for hosting a merchant's e-commerce website and its associated databases.
(B) A standardized paper agreement signed manually by transacting parties to ensure legal enforceability.
(C) An ordered sequence of bits with a unique identification representing a collection of operations and information.
(D) An independent third party operating as a neutral intermediary between financial agents during a settlement.

May/June 2005

**13.** What is the primary function of Payment Orchestration?
(A) Connecting payment processors and gateways to provide a platform for enabling and optimizing payments.
(B) Delivering electronic bills to a centralized web site to facilitate one-stop shopping for the consumer.
(C) Allowing consumers to spread payments over a set period of time at the physical checkout counter.
(D) Embedding digital payment options within non-finance apps to reduce customer checkout friction.

Oct/Nov 2022

**14.** During the e-commerce activity of negotiating, which of the following actions is typically undertaken by buyers and sellers?
(A) Issuing a contractual agreement setting forth the exact quantity and the agreed-upon unit price.
(B) Resolving mistakes concerning product quality and the physical delivery of items to the buyer.
(C) Determining exchange terms, such as delivery, refund policies, and arranging for payment credit.
(D) Reconciling electronic transactions in accounts receivable and payable within the accounting system.

May/June 2018

**15.** Which statement correctly describes the goal of Universal Queuing in a call center?
(A) It routes outbound calls using automated predictive dialers.
(B) It replaces traditional telephony with internet protocol networks exclusively.

Downloaded from www.pdf.tube

# CHAPTER 12

# E-Commerce and E-Banking

May/June 2016

**1.** Which standard is sponsored by W3C for electronic business?
(A) OBI
(B) OFX
(C) OTP
(D) JEPI

Oct/Nov 2009

**2.** What does the "open-loop" characteristic in Real-Time Payments indicate?
(A) Payments rely strictly on a prepaid balance to accelerate the process.
(B) Payments occur exclusively between two different mobile network operators.
(C) Payments are directly connected to personal accounts instead of relying on a prepaid balance.
(D) Payments are restricted to specific geographies and local currencies.

May/June 2023

**3.** How is Mobile Payment defined?
(A) The delivery of digital goods exclusively using electronic email networks.
(B) The process of resolving mistakes or complaints concerning product quality via mobile phones.
(C) Financial-regulated payment services performed from or through a mobile device.
(D) An electronic network exclusively used for large corporate financial settlements.

Oct/Nov 2018

**4.** Which statement correctly describes the MNO-centric mobile payment model?
(A) The bank handles the mobile payments while the MNO provides only the air connection.
(B) A third party operates as a neutral intermediary between financial agents.
(C) The MNO does the billing either on the prepaid user account or later on the phone bill.
(D) The merchant and his agent handle interactions with the mobile device entirely.

May/June 2007

**5.** Which concept fundamentally deals with customer self-service, personalized offerings by analyzing past customer behaviour, and anticipating wants and needs?
(A) Collaborative Forecasting and Replenishment
(B) Customer Relationship Management
(C) Supply Chain Management
(D) Electronic Bill Presentment

Oct/Nov 2025

**6.** Which statement is true regarding the Hybrid model in Electronic Bill Presentment and Payment (EBPP)?
(A) The company manages and controls the entire billing process without any third party.
(B) The billing company sends bill summary data to the consolidator while retaining bill detail information at their own Web site.
(C) An on-line consolidation firm fully manages the detailed bill presentation for the billing company.
(D) The bill is reduced to a single line item without any possibility of customer interaction.

May/June 2012

How is E-business defined in the context of organizational operations?
(A) It is the electronic presentation of retail goods and services designed primarily for facilitating online consumer ordering.
(B) It is the electronic sharing of structured or unstructured business information among suppliers, customers, and partners.
(C) It is a technological framework consisting of procurement, forecasting, and inventory management systems used within a firm.
(D) It is the ability to perform commercial transactions involving the physical exchange of tangible goods using electronic tools.

NODIA

**Oct/Nov 2024**

**24.** Which statement correctly identifies existing APIs and information exchange protocols used for digital object operations?
(A) ACD, IVR, and WFM
(B) SCM, CRM, and ERP
(C) OBI, JEPI, and OFX
(D) FTP, HTTP, SMTP, and MIME

**May/June 2017**

**25.** How does a screen pop function within Computer Telephony Integration (CTI)?
(A) It automatically dials numbers from a database list and detects busy signals or voicemail.
(B) It displays a customer's profile automatically using ANI or a front-end identification request.
(C) It pools all customers on hold into a single waiting list across multiple communication channels.
(D) It employs speech recognition and mood detection algorithms to handle routine customer inquiries.

**Oct/Nov 2005**

**26.** What is the definition of a push message in SMS banking?
(A) A message initiated by the customer using a mobile phone to request current account balance or statement information.
(B) A secure protocol used for transferring high-value funds between two different commercial banking institutions.
(C) A message utilized exclusively to establish a new online banking password or to reset a locked user account.
(D) A bank-initiated message sent to a customer's mobile phone without a prior request for that specific information.

**May/June 2020**

**27.** Which statement accurately reflects a feature of Banking Alerts?
(A) They are notifications about transactional activities delivered to the customer via SMS.
(B) They require the customer to initiate a text message to receive an update.
(C) They cannot be customized via the Online Banking website.
(D) They are exclusively used for combating cyber fraud through OTPs.

**Oct/Nov 2015**

**28.** In which year was the first patent that solely defined "Mobile Payment System" filed?
(A) 1995
(B) 1998
(C) 2000
(D) 2005

**May/June 2013**

**29.** Which of the following is a direct benefit of E-commerce?
(A) Increasing float through delayed payment processing.
(B) Eliminating the need for any network system or domain name registration.
(C) Reducing the economic distance between producers and consumers.
(D) Restricting the marketplace to local and regional boundaries.

**Oct/Nov 2021**

**30.** In the context of mobile payment models, what characterizes the Independent Service Provider (ISP) model?
(A) The bank handles payments while the mobile network operator provides the necessary air connection.
(B) The mobile network operator manages all transactions and billing on the monthly phone bill.
(C) The merchant and agent handle all interactions directly with the mobile device and its software.
(D) A trusted third party operates as a neutral intermediary between financial agents and operators.

**May/June 2024**

**31.** Which statement about Cross-Selling Services in Call Centers is incorrect?
(A) Call centers that consistently cross-sell can quickly become a profit center.
(B) Each time an agent resolves a customer issue is the time to probe for a cross-sell opportunity.
(C) Cross-selling transforms the call center strictly into an absolute cost-center.
(D) It is a productive and cost-effective means of selling services to new and existing customers.

Click Here to Buy book on Amazon

Oct/Nov 2011

**64.** Consider the following statements about the Bharat Bill Payment System (BBPS):
1. It is an integrated bill payment system offering interoperable and accessible bill payment service.
2. It is driven by the RBI but conceptualised by the IDRBT.
3. It supports multiple payment modes including NEFT Internet Banking, UPI, and Cash.

Which combination of the statements is correct?
(A) 1 and 2 only
(B) 2 and 3 only
(C) 1 and 3 only
(D) 1, 2, and 3

May/June 2010

**65.** Identify the correct pair matching the e-business standard to its primary function.
(A) OBI - For purchasing customers
(B) OFX - For financial institutions
(C) OTP - Sponsored by W3C
(D) JEPI - For high volume low-cost transactions

Oct/Nov 2024

**66.** Consider the following call center benchmarks and measurements:
1. Abandonment Rates should be less than 2%.
2. Number of Calls per Agent is targeted at 200 per Day.
3. Average Speed of Answer should be 20 Seconds.
4. Percentage of Blocked Calls (Busy) should be more than 10%.

Which combination of the statements is correct?
(A) 1, 2, and 4 only
(B) 2, 3, and 4 only
(C) 1, 2, and 3 only
(D) 1, 3, and 4 only

May/June 2017

**67.** The following are steps involved in the Consolidated Bill process:
1. Select and view the desired bill's detail.
2. Sign on to email box for entering password.
3. Click the payment hyperlink and approve payment.
4. Open and read an e-mail message announcing that a bill has been presented.
5. Access on Internet.

Which of the following represents the correct chronological sequence?
(A) 5, 2, 4, 1, 3
(B) 5, 4, 2, 1, 3
(C) 2, 5, 1, 4, 3
(D) 1, 2, 3, 4, 5

Oct/Nov 2005

**68.** Consider the following statements:
1. Computer Telephony Integration (CTI) often utilizes Screen Pops in tandem with a unified desktop to provide agents with customer data.
2. Automatic Call Distributor (ACD) is a telephony system that recognizes, answers, and routes incoming calls to the most suitable terminal.

Which of the following combinations is correct?
(A) Both 1 and 2 are correct
(B) Only 1 is correct
(C) Only 2 is correct
(D) Both 1 and 2 are incorrect

May/June 2020

**69.** Consider the following statements regarding the differences between mobile banking and mobile payments:
1. In mobile banking, money can be transferred only when the account number of the payee is known beforehand.
2. In mobile payments, the account number is masked from being public.
3. The necessity of the bank account number for simple transactions like paying auto fare is identical in both systems.

Which combination of the statements is correct?
(A) 1, 2, and 3
(B) 1 and 2 only
(C) 2 and 3 only
(D) 1 and 3 only

Oct/Nov 2015

**70.** Match the call center technologies in List I with their characteristics in List II.
List I: (Call Center Technologies)
P. Predictive Dialer
Q. Voice Biometrics
R. CRM Servicing Application
S. Campaign Management System
List II: (Characteristics)
1. Gives agents 360-degree customer info and documents interactions
2. Helpful for outbound call centers, providing

NODIA

May/June 2022

**41.** The following steps are involved in enabling e-commerce:

1. Accept electronic payment methods for full transaction shopping or bill payment.
2. Move static billing statement data to an interactive web-based presentment server.
3. Develop a dynamic, database-driven online catalogue.
4. Provide online ordering by securely integrating your front-end presentation with an order entry system.

Which of the following represents the correct chronological sequence?

(A) 3, 4, 2, 1
(B) 1, 2, 3, 4
(C) 4, 3, 1, 2
(D) 2, 4, 1, 3

Oct/Nov 2023

**42.** Which of the following statements about One-Time Passwords (OTPs) is incorrect?

(A) They are used by financial institutions to combat cyber fraud.
(B) They are sent to a customer's mobile phone via SMS.
(C) They remain valid indefinitely until the customer completes the transaction.
(D) They replace traditional memorized passwords for completing online transactions.

May/June 2016

**43.** Which of the following is NOT listed as a standard Call Center Benchmark?

(A) Abandonment Rates
(B) Number of Software Agents deployed
(C) Average Speed of Answer
(D) Number of Calls per Agent

Oct/Nov 2009

**44.** Which of the following is NOT considered a key activity in electronic commerce?

(A) Advertising and shopping
(B) Negotiating
(C) Distribution and receipt
(D) Manual cheque truncation

May/June 2023

**45.** What is the primary reason merchants actively drive the shift toward mobile wallets?

(A) To mandate paper receipts for every digital transaction.
(B) To restrict younger consumers from completing online purchases.
(C) To avoid the hefty card swipe fees levied by major credit card companies.
(D) To eliminate the need for cybersecurity solutions at the point of sale.

Oct/Nov 2018

**46.** Which of the following is an incorrect statement regarding the White label model?

(A) It involves the setting up of a branded online store managed by the e-Commerce player or a third party.
(B) The brand avoids taking responsibility for generating website traffic and providing services.
(C) It partners with payment gateways to provide services.
(D) It helps build trust, customer affinity, and loyalty.

NODIA

May/June 2007

**47.** What is the greatest advantage for a billing company using the biller direct model combined with consolidators for summary information?

(A) The bill is reduced to a single line item, freeing up server space.
(B) The billing company retains full control over the bill detail data and customer interaction to leverage targeted advertising and cross-selling.
(C) The consolidator assumes all transaction costs associated with delivering bills.
(D) The customer completely avoids visiting the biller's site for any detailed review.

Oct/Nov 2025

**48.** Which statement incorrectly identifies a feature of the pure Consolidator model in EBPP?

(A) An on-line consolidation firm manages the process for the billing company.
(B) The billing company gains maximum opportunity to establish and maintain a personal, direct relationship with each customer.
(C) The ultimate goal is to allow customers to review and pay all their bills with one-stop-shopping convenience.
(D) The bill may be reduced to a single line item on a consolidated page.

May/June 2012

**49.** Which of the following is NOT a supported payment mode under the Bharat Bill Payment System (BBPS)?
(A) International Letters of Credit
(B) NEFT Internet Banking
(C) Cards (Credit, Debit and Prepaid)
(D) Aadhaar based Payments

Oct/Nov 2014

**50.** Which of the following is NOT a primary model for mobile payments?
(A) Bank-centric model
(B) Operator-centric model
(C) Logistics-centric model
(D) Independent service provider (ISP) model

May/June 2019

**51.** What is the most significant impact of embedded payments on the user experience?
(A) They introduce multiple redirection screens to ensure maximum payment security.
(B) They mandate the use of traditional banking portals for every non-finance app transaction.
(C) They prevent merchants from harnessing customer data at the point of purchase.
(D) They deliver a frictionless purchase journey by allowing merchants to accept payments natively within non-payment apps.

Oct/Nov 2006

**52.** Which statement incorrectly characterizes Time Division Multiplexing (TDM) and Internet Protocol (IP) in call centers?
(A) TDM transports call center interactions by segmenting multiple data streams into a single signal.
(B) IP offers easy access and value-added services such as instant messaging and video calling.
(C) IP allows moving through a less costly network while making phone calls directly from websites.
(D) TDM has largely replaced IP as the primary mechanism for transporting call center transactions.

May/June 2021

**53.** Which of the following is NOT an essential step required to enable e-commerce?
(A) Develop a dynamic, database-driven online catalogue.
(B) Move static billing statement data to an interactive web-based presentment server.
(C) Restrict electronic payment methods exclusively to offline cheque clearing.
(D) Provide online ordering by securely integrating front-end presentation with an order entry system.

Oct/Nov 2010

**54.** What is the main reason organizations are prioritizing omnichannel support in their call centers?
(A) It eliminates the need for any human agents by relying entirely on Interactive Voice Response.
(B) It forces customers to resolve all issues exclusively through the mobile application.
(C) Customers expect a consistent, personalized, and relevant experience regardless of the channel they interact through.
(D) It reduces the required technology infrastructure to a single telephone line.

May/June 2005

**55.** Which of the following is NOT an example of a typical push service in SMS banking?
(A) Foreign currency exchange rates enquiry
(B) Periodic account balance reporting at the end of the month
(C) An alert that an e-statement is ready to be downloaded
(D) Successful payment of a cheque issued on the account

Oct/Nov 2022

**56.** Which statement incorrectly describes the Acquirer-Centric mobile payment model?
(A) The customer and his agent are exclusively in charge of handling the interaction with the mobile device.
(B) The merchant and his agent are in charge of handling interactions with the mobile device.
(C) It is contrasted with the issuer-centric model in terms of who handles the interactions.
(D) It dominates specific existing mobile payment efforts in the market.

May/June 2018

**57.** What is the core advantage of Buy Now, Pay Later (BNPL) products that makes them highly appealing to consumers?

Downloaded from www.pdf.tube

(A) They provide credit decisions in minutes, are easier to obtain than traditional credit, and offer manageable installment options often at no interest.
(B) They require a complex, multi-day credit approval process ensuring high security.
(C) They mandate high interest charges on upfront payments protecting merchant margins.
(D) They restrict purchases exclusively to healthcare products globally.

**Oct/Nov 2016**

**58.** Which statement incorrectly describes Real-Time Payments (RTP)?
(A) Payments rely strictly on a closed-loop prepaid balance to accelerate the process.
(B) The idea is to complete the process of initiating, clearing, and settling the payment in a matter of seconds.
(C) Real-time payment networks ideally work 24 x 7 x 365.
(D) Banks need to provide 24 x 7 backend systems to leverage RTP.

**May/June 2014**

**59.** What is the primary goal of implementing Universal Queuing in a call center?
(A) To record all customer interactions historically or in real-time.
(B) To segment multiple data streams and put them in a single telephony signal.
(C) To pool all customers on hold into a single waiting list, regardless of the contact channel used.
(D) To automatically dial from a list of phone numbers and detect busy signals.

**Oct/Nov 2007**

**60.** Which of the following is NOT classified as a type of software agent in e-commerce building blocks?
(A) Translators
(B) Treasury bills and bonds
(C) Escrow agents
(D) Workflow managers

**May/June 2025**

**61.** Match the mobile payment models in List I with their characteristics in List II.
List I: (Mobile Payment Models)
P. Acquirer-Centric
Q. Issuer-Centric
R. Bank-Centric
S. MNO-Centric
List II: (Characteristics)
1. The merchant may be totally unaware of the mobile nature of the payment
2. The network operator does the billing either on the prepaid account or later on the phone bill
3. The merchant and his agent handle interactions with the mobile device
4. The financial institution handles payments while the network operator only provides the air connection
(A) P-3, Q-1, R-4, S-2
(B) P-1, Q-4, R-2, S-3
(C) P-3, Q-4, R-1, S-2
(D) P-4, Q-2, R-3, S-1

NODIA

**Oct/Nov 2019**

**62.** Consider the following statements:
1. The pure consolidator model allows the billing company to easily tailor bill presentation and retain sensitive customer data locally.
2. The biller direct model allows customers to review and pay all their bills from multiple billers with one-stop-shopping convenience.
Which of the following combinations is correct?
(A) Both 1 and 2 are correct
(B) Only 1 is correct
(C) Only 2 is correct
(D) Both 1 and 2 are incorrect

**May/June 2009**

**63.** Match the e-business standards in List I with their appropriate descriptions in List II.
List I: (E-business Standards)
P. OBI
Q. JEPI
R. OFX
S. OTP
List II: (Descriptions)
1. For purchasing customers
2. Sponsored by W3C
3. For financial institutions
4. For high volume low-cost transactions
(A) P-2, Q-3, R-1, S-4
(B) P-4, Q-2, R-3, S-1
(C) P-3, Q-1, R-4, S-2
(D) P-1, Q-4, R-2, S-3

(C) It authenticates a person's identity using unique vocal patterns.
(D) It pools all customers on hold into a single waiting list, regardless of the contact channel.

**Oct/Nov 2016**

**16.** What is the definition of Electronic Commerce?
(A) The exchange of goods or services between two or more parties using electronic tools and techniques to perform transactions.
(B) A set of internal processes consisting of procurement, inventory management, forecasting, and automated warehousing.
(C) The electronic delivery of a bill or bill-equivalent document, excluding the actual generation of the underlying data.
(D) A telephony system that recognizes, answers, and routes incoming customer calls to the most appropriately suited terminal.

**May/June 2014**

**17.** Which of the following is an approach for E-banking implementation?
(A) Develop a sound business case to chart the e-business investment.
(B) Revert to traditional paper-based processes for high-value clients.
(C) Compete directly with the underlying business instead of complementing it.
(D) Avoid developing other non-bank financial services over time.

**Oct/Nov 2007**

**18.** According to industry Call Center Benchmarks, what is the target percentage for Blocked Calls (Busy)?
(A) Less than 5%
(B) Less than 2%
(C) Less than 1%
(D) Less than 10%

**May/June 2025**

**19.** How do embedded payments function in the digital ecosystem?
(A) They route incoming customer service calls to the most suitable terminal.
(B) They consolidate multiple utility bills into a single electronic presentment portal.
(C) They generate one-time passwords for secure mobile banking authentication.
(D) They allow non-finance or non-fintech merchants to accept payments within non-payment apps.

**Oct/Nov 2019**

**20.** What is the fundamental difference between mobile banking and mobile payments?
(A) Mobile payments mask the account number from the public, whereas mobile banking requires a known payee account number.
(B) Mobile banking requires high-speed internet access, whereas mobile payments only use localized hardware connectivity.
(C) Mobile payments require the payee's account number to be registered beforehand, unlike standard mobile banking.
(D) Mobile banking involves the total absenteeism of the bank account number, while mobile payments strictly require it.

**May/June 2009**

**21.** Which statement correctly describes the transaction initiation capabilities of Bharat BillPay?
(A) Transactions can only be initiated through Internet Banking and Mobile Wallets.
(B) Transactions are restricted to credit cards and cash only.
(C) Transactions can be initiated through multiple payment channels including POS, ATM, Bank Branch, and Agents.
(D) Transactions exclude NEFT and UPI channels entirely.

**Oct/Nov 2011**

**22.** What are the three dimensions in which e-business is carried out?
(A) B2B, B2C, and C2C
(B) SCM, CRM, and E-commerce
(C) Procurement, Warehousing, and Logistics
(D) Advertising, Negotiating, and Ordering

**May/June 2010**

**23.** Which process is primarily concerned with customized extranet sites, web servers, and groupware to manage procurement, forecasting, and logistics?
(A) Customer Relationship Management
(B) Universal Queuing Matrix
(C) Payment Orchestration
(D) Supply Chain Management

Click Here to Buy book on Amazon

agents with contact lists
3. Automatically dials from a list of phone numbers detecting busy signals
4. Authenticates a person's identity to prevent fraud

(A) P-3, Q-4, R-1, S-2
(B) P-1, Q-4, R-2, S-3
(C) P-4, Q-2, R-3, S-1
(D) P-3, Q-1, R-4, S-2

**May/June 2013**

**71.** Consider the following statements about Real-Time Payments (RTP):
1. They initiate, clear, and settle the payment in a matter of seconds.
2. Real-time payment networks work 24 x 7 x 365.
3. They are strictly defined by a "closed-loop" architecture.
4. They require banks to provide 24 x 7 backend systems.

Which combination of the statements is correct?
(A) 1, 2, and 4 only
(B) 1, 3, and 4 only
(C) 2, 3, and 4 only
(D) 1, 2, and 3 only

**Oct/Nov 2021**

**72.** Match the innovative online business models in List I with their descriptions in List II.
List I: (Online Business Models)
P. Marketplace and pick-up & drop
Q. Self-owned inventory
R. Private label
S. White label
List II: (Descriptions)
1. The brand takes responsibility for generating website traffic and providing services by partnering with payment gateways
2. Sellers partner with leading platforms to set up a dedicated online store, managing inventory but having limited say on pricing
3. E-commerce company sets up its own brand goods competing with branded labels
4. E-Commerce player possesses the stock, providing smoother operations but risking potential mark downs

(A) P-2, Q-4, R-3, S-1
(B) P-1, Q-4, R-2, S-3
(C) P-3, Q-1, R-4, S-2
(D) P-4, Q-2, R-3, S-1

**May/June 2024**

**73.** Consider the following statements regarding Computer Telephony Integration (CTI):
1. CTI often utilizes Screen Pops in tandem with a unified desktop to provide agents with customer data.
2. Automatic Call Distributor (ACD) is a telephony system that recognizes, answers, and routes incoming calls to the most suitable terminal.

Which of the following combinations is correct?
(A) Both 1 and 2 are correct
(B) Only 1 is correct
(C) Only 2 is correct
(D) Both 1 and 2 are incorrect

**Oct/Nov 2008**

**74.** Identify the correct pair matching the type of payment based on value to its typical amount.
(A) Micro-Payments - Typically more than $20
(B) Mini-Payments - Typically under $2
(C) Mini-Payments - Between $2 and $20
(D) Macro-Payments - Typically under $20

**May/June 2006**

**75.** Consider the following statements regarding payments based on value:
1. Micro-Payments are typically under $2.
2. Mini-Payments target commonly purchased small items between $2 and $20.
3. Macro-Payments are typically more than $20.
4. Prepayments for mobile micro payments decrease processing costs as transaction numbers decrease.

Which combination of the statements is correct?
(A) 1, 2, and 3 only
(B) 1, 3, and 4 only
(C) 2, 3, and 4 only
(D) 1, 2, 3, and 4

**Oct/Nov 2017**

**76.** Match the dimensions of E-business in List I with their primary purpose in List II.
List I: (Dimensions of E-business)
P. SCM
Q. CRM
R. E-commerce
S. Groupware
List II: (Primary Purpose)
1. Bringing Customers and Associates closer
2. E-mail-integrated collaborative software

NODIA

Oct/Nov 2007

**102.** Consider the following technologies implemented in Call Centers:
1. Computer Telephony Integration (CTI)
2. Interactive Voice Response (IVR)
3. Workforce Management Software (WFM)
4. Quality Management (QM)
5. Electromagnetic Pulse Mitigation (EPM)

Which of the following combinations correctly identifies the listed Call Center technologies?
(A) 1, 2, 3, and 5 only
(B) 2, 3, 4, and 5 only
(C) 1, 2, 3, and 4 only
(D) 1, 2, 4, and 5 only

May/June 2025

**103.** To ensure the optimal number of agents are hired to keep average wait times low, Apex Bank implements a system that uses historical interactions to predict future call volumes. Which software solution provides these forecasting capabilities?
(A) Quality Management (QM)
(B) Workforce Management Software (WFM)
(C) Administration Console
(D) Voice Biometrics Engine

Oct/Nov 2019

**104.** Each of the following questions consists of two statements, one labeled as Assertion (A) and the other as Reason (R). Select the correct answer from the options given below.
Assertion (A): The pure consolidator model provides the billing company with maximum opportunity to establish and maintain a personal, direct relationship with each customer.
Reason (R): In the consolidator model, the customer's bill may be reduced to a single line item on a consolidated page.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2009

**105.** Nexus Bank also offers an SMS service where a customer's phone automatically receives an alert message if a withdrawal exceeding $500 occurs at any ATM. What type of SMS service is this?
(A) Mini statement request
(B) Pull message
(C) Push message
(D) Stop payment instruction

Oct/Nov 2011

**106.** Consider the following typical push services in SMS banking:
1. Periodic account balance reporting
2. Large value withdrawals on an account
3. One-time password for authentication
4. Foreign currency exchange rates enquiry
5. An alert that an e-statement is ready to be downloaded

Which of the following accurately represents the combination of push services?
(A) 1, 2, 3, and 5 only
(B) 1, 3, 4, and 5 only
(C) 2, 3, 4, and 5 only
(D) 1, 2, 3, 4, and 5

May/June 2010

**107.** Suppose Zenith Retail decided instead to launch an online store branded under their name, but the platform management, website traffic generation, and payment gateway partnerships were entirely handled by a third-party technology provider. Which business model would this represent?
(A) White label
(B) Self-owned inventory
(C) Private label
(D) Independent Service Provider

Oct/Nov 2024

**108.** Each of the following questions consists of two statements, one labeled as Assertion (A) and the other as Reason (R). Select the correct answer from the options given below.
Assertion (A): Digital objects are easily created, reused, and modified with minimal side effects.
Reason (R): Digital objects can be specified and accessed in an application-independent manner.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.

Downloaded from www.pdf.tube

(C) P-3, Q-1, R-4, S-2
(D) P-4, Q-2, R-3, S-1

**May/June 2022**

**83.** Match the emerging digital payment trends in List I with their characteristics in List II.
List I: (Digital Payment Trends)
P. Buy Now, Pay Later (BNPL)
Q. Mobile Wallets
R. Payment Orchestration
S. Real-Time Payments
List II: (Characteristics)
1. Adopts an open-loop model directly connected to personal accounts
2. Smartphone apps sparking a snowball effect in contactless payments
3. Allows customers to spread payments over a set period of time, often at no interest
4. Connects multiple processors and gateways to provide a one-stop-shop platform
(A) P-3, Q-2, R-4, S-1
(B) P-1, Q-4, R-2, S-3
(C) P-4, Q-2, R-3, S-1
(D) P-3, Q-1, R-4, S-2

**Oct/Nov 2023**

**84.** Consider the following statements regarding SMS Banking Security:
1. The lack of encryption is inherent to the SMS banking channel.
2. Several banks have overcome fears by introducing compensating controls.
3. Security tokens and pre-registration are typical methods employed where transaction risk is perceived to be high.
Which combination of the statements is correct?
(A) 1 and 2 only
(B) 2 and 3 only
(C) 1, 2, and 3
(D) 1 and 3 only

**May/June 2016**

**85.** Consider the following statements:
1. Push messages are initiated by the customer using a mobile phone for obtaining information.
2. Pull messages are those that a bank sends out to a customer's mobile phone without a customer request.
Which of the following combinations is correct?
(A) Both 1 and 2 are correct
(B) Only 1 is correct
(C) Only 2 is correct
(D) Both 1 and 2 are incorrect

**Oct/Nov 2009**

**86.** Match the E-commerce activities in List I with their functions in List II.
List I: (E-commerce Activities)
P. Ordering
Q. Billing
R. Payment and Settlement
S. Distribution and Receipt
List II: (Functions)
1. Remittance information is analyzed by the seller and accepted as valid
2. Issuing a contractual agreement of the terms of exchange and payment
3. Seller provides proof or arranges delivery of purchased goods
4. Sending remittance information that should accompany the payment
(A) P-4, Q-2, R-3, S-1
(B) P-1, Q-4, R-2, S-3
(C) P-2, Q-4, R-1, S-3
(D) P-3, Q-1, R-4, S-2

NODIA

**May/June 2023**

**87.** Consider the following components for starting e-commerce activities:
1. A server to host site
2. A network system
3. Domain name registration for the site
4. Purely manual order entry architecture
Which combination of the statements is correct?
(A) 1, 2, and 4 only
(B) 1, 2, and 3 only
(C) 2, 3, and 4 only
(D) 1, 3, and 4 only

**Oct/Nov 2018**

**88.** Match the EBPP concepts in List I with their descriptions in List II.
List I: (EBPP Concepts)
P. Biller direct model
Q. Consolidator model
R. Hybrid model
S. Pre-delivery float time
List II: (Descriptions)
1. Billing company sends bill summary data to a third party while retaining bill detail information at their own site
2. Time between when the bill data is available and the customer's actual receipt of the bill

3. Streamlining Internal Business processes
4. On-line purchase

(A) P-3, Q-1, R-4, S-2
(B) P-1, Q-4, R-2, S-3
(C) P-3, Q-4, R-1, S-2
(D) P-4, Q-2, R-3, S-1

**May/June 2008**

**77.** Consider the following statements regarding Chatbots in Call Centers:

1. They are known as conversational AI and can recognize multiple languages.
2. They use Natural Language Processing (NLP) to determine the customer's intent.
3. They completely replace the need for traditional Interactive Voice Response (IVR) systems.

Which combination of the statements is correct?

(A) 1 and 3 only
(B) 1 and 2 only
(C) 2 and 3 only
(D) 1, 2, and 3

**Oct/Nov 2013**

**78.** Match the call center technologies in List I with their primary functions in List II.

List I: (Call Center Technologies)

P. CTI
Q. ACD
R. Intelligent Call back
S. Universal Queuing

List II: (Primary Functions)

1. Allows callers to select an option to be contacted later instead of waiting in a queue
2. Pools all customers on hold into a single waiting list regardless of contact channel
3. Enables computer and telephone systems to interact, providing screen pops to agents
4. Recognizes, answers, and routes incoming calls to the best suited terminal or agent

(A) P-3, Q-4, R-1, S-2
(B) P-1, Q-4, R-2, S-3
(C) P-4, Q-2, R-3, S-1
(D) P-2, Q-3, R-1, S-4

**May/June 2015**

**79.** Consider the following statements:

1. Buy Now, Pay Later (BNPL) technologies proliferated during the pandemic and offer alternatives to traditional credit cards.
2. Payment Orchestration simplifies global payments by utilizing real-time analytics and AI-based intelligent routing.

Which of the following combinations is correct?

(A) Both 1 and 2 are correct
(B) Only 1 is correct
(C) Only 2 is correct
(D) Both 1 and 2 are incorrect

**Oct/Nov 2012**

**80.** Identify the incorrect pair regarding Banking and Credit Card Alerts.

(A) Bounced cheque - Credit Card Related Alert
(B) Local or Overseas ATM Cash Withdrawal - Banking Related Alert
(C) Credit Limit Nearing Maximum - Credit Card Related Alert
(D) Past Due Date Reminder - Credit Card Related Alert

**May/June 2011**

**81.** Consider the following statements regarding the benefits of Electronic Billing Systems:

1. They require tremendous investment in physical printing and assembly.
2. They reduce the value lost in uncollected receipts during pre-delivery float time.
3. They enable sophisticated personalization with targeted messages based on specific customer knowledge.
4. They assist in migrating customers from lower-cost channels to higher-cost paper-based channels.

Which combination of the statements is correct?

(A) 1 and 4 only
(B) 2 and 3 only
(C) 1, 2, and 3 only
(D) 2, 3, and 4 only

**Oct/Nov 2020**

**82.** Match the classes of digital objects in List I with their examples in List II.

List I: (Classes of Digital Objects)

P. Unstructured information
Q. Structured information
R. Objects for sale
S. Agents and brokers

List II: (Examples)

1. Software objects, movies/videos
2. Reports and freeform text, voice, and video
3. Information filters, trusted third parties
4. EDI messages, electronic forms

(A) P-2, Q-4, R-1, S-3
(B) P-1, Q-4, R-2, S-3

Click Here to Buy book on Amazon

Reason (R): Predictive dialers require agents to manually listen to every dialing sequence to verify the connection quality.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2010**

**96.** A customer traveling abroad wants to know the latest foreign currency exchange rates and sends an SMS request to Nexus Bank. The bank responds with the rates. This interaction is an example of which SMS banking functionality?
(A) Periodic account balance reporting
(B) Pull service
(C) Push service
(D) Un-successful execution of a standing order

**May/June 2005**

**97.** Consider the following key activities in electronic commerce:
1. Advertising and shopping
2. Negotiating
3. Ordering
4. Billing
5. Payment and settlement

Which of the following represents the correct combination of these activities?
(A) 1, 2, 4, and 5 only
(B) 1, 2, 3, and 5 only
(C) 2, 3, 4, and 5 only
(D) 1, 2, 3, 4, and 5

**Oct/Nov 2022**

**98.** Read the following scenario and answer the questions that follow:
*Apex Bank is upgrading its customer service division to better handle high volumes. The system automatically identifies the caller's telephone number and pulls up the customer's profile on the agent's screen as soon as the call connects.*
Which specific feature of Computer Telephony Integration (CTI) is primarily responsible for identifying the telephone number?
(A) Automated Number Identification (ANI)
(B) Designated Number Identification (DNI)
(C) Predictive Dialer Output
(D) Interactive Voice Response (IVR)

**May/June 2018**

**99.** To manage their invoicing, Zenith Retail implements a system where they send summary bill data to a popular third-party payment portal. However, customers must visit Zenith's own website to view the detailed breakdown of the bill. Which Electronic Bill Presentment and Payment (EBPP) model is being utilized?
(A) Biller direct model
(B) Hybrid model
(C) Consolidator model
(D) Operator-centric model

**Oct/Nov 2016**

**100.** Each of the following questions consists of two statements, one labeled as Assertion (A) and the other as Reason (R). Select the correct answer from the options given below.
Assertion (A): In mobile payments, one need not know the account number of a person to transfer money.
Reason (R): The account number is completely masked from being public in mobile payment architecture.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2014**

**101.** Nexus Bank's marketing campaign highlights that users of their new mobile payment app can transfer money to friends to split a taxi fare without ever needing to ask for or input their friend's bank account number. Which conceptual difference does this highlight between mobile payments and traditional mobile banking?
(A) The total absenteeism and masking of the bank account number in mobile payments.
(B) The requirement of localized proximity connections via RF for all transactions.
(C) The necessity of using macro-payments for simple peer-to-peer transfers.
(D) The mandatory generation of physical receipts for all mobile payment transactions.

Downloaded from www.pdf.tube

(A) Universal Queuing Matrix
(B) Campaign Management System (CMS)
(C) Customer Relationship Management (CRM)
(D) Automatic Call Distributor (ACD)

**Oct/Nov 2008**

**116.** Consider the following features of Contracts as digital objects:
1. They include instructions regarding handling, routing, storing, and scheduling.
2. They can be negotiated, including prices and terms of payment.
3. They can be written, signed, read, and amended.
4. In the case of electronic cash, they can easily be altered, reproduced, or copied.
5. They can be bought, sold, and exchanged in many instances.

Which of the following correctly represents the features of Contracts?
(A) 1, 2, 3, and 5 only
(B) 1, 2, 4, and 5 only
(C) 2, 3, 4, and 5 only
(D) 1, 2, 3, 4, and 5

**May/June 2006**

**117.** Read the following scenario and answer the questions that follow:
*Nexus Bank has partnered with a prominent telecom operator to launch a micropayment service. When a user buys a digital song, the telecom operator charges the transaction directly to the user's monthly phone bill rather than deducting it from a bank account.*
Which mobile payment model does this scenario represent?
(A) Bank-centric model
(B) Independent service provider (ISP) model
(C) Collaborative model
(D) MNO-centric model

**Oct/Nov 2017**

**118.** Each of the following questions consists of two statements, one labeled as Assertion (A) and the other as Reason (R). Select the correct answer from the options given below.
Assertion (A): Banks completely abandoned SMS banking due to the inherent lack of encryption in SMS messages.
Reason (R): Banks that use SMS banking have introduced compensating controls and limited the application's scope to mitigate security risks.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2008**

**119.** Read the following scenario and answer the questions that follow:
*Zenith Retail wants to aggressively expand its online presence. Instead of solely relying on third-party products, they decide to manufacture and sell their own brand goods directly through their website to secure higher profit margins.*
Which online business model is Zenith Retail employing?
(A) Private label
(B) Marketplace and pick-up & drop
(C) White label
(D) Consolidator model

**Oct/Nov 2013**

**120.** Each of the following questions consists of two statements, one labeled as Assertion (A) and the other as Reason (R). Select the correct answer from the options given below.
Assertion (A): Real-time payment systems rely strictly on prepaid balances to guarantee that payments clear in a matter of seconds.
Reason (R): Real-time payments feature an "open-loop" characteristic directly connected to personal accounts.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2015**

**121.** A popular food delivery app utilizes FinNova's APIs to allow customers to finalize payments seamlessly within the app's own checkout page, without being redirected to an external banking site. This capability is specifically referred to as:
(A) Mobile Wallet synchronization

NODIA

(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2017**

**109.** During operations, Apex Bank notices some agents are not adhering to scheduled break times, causing unexpected spikes in customer wait queues. Which application should the managers use to identify areas of weakness and ensure adherence to internal policies?
(A) Campaign Management System (CMS)
(B) Interactive Video (IV)
(C) Predictive Dialer
(D) Quality Management (QM)

**Oct/Nov 2005**

**110.** Each of the following questions consists of two statements, one labeled as Assertion (A) and the other as Reason (R). Select the correct answer from the options given below.
Assertion (A): Payment providers are investing heavily in new cybersecurity solutions such as behavioral biometrics.
Reason (R): The rise of e-commerce and non-cash payments has led to a jump in cyber threats.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2020**

**111.** To mitigate security risks for high-value fund transfers, Nexus Bank stops relying on traditional static passwords and instead sends a secure, short-lived code via SMS that the user must input to complete the transaction. What is this security mechanism called?
(A) Voice Biometrics
(B) Screen Pop
(C) Automated Number Identification (ANI)
(D) One-Time Password (OTP)

**Oct/Nov 2015**

**112.** Each of the following questions consists of two statements, one labeled as Assertion (A) and the other as Reason (R). Select the correct answer from the options given below.
Assertion (A): E-business is defined purely as a destination to reach a digital marketplace endpoint.
Reason (R): E-business is drastically transforming the way we live and work today.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2013**

**113.** Each of the following questions consists of two statements, one labeled as Assertion (A) and the other as Reason (R). Select the correct answer from the options given below.
Assertion (A): The Reserve Bank of India (RBI) has made SMS alerts mandatory for clearing cheque transactions.
Reason (R): There was an increasing concern over the rise in cheque-related fraud cases.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2021**

**114.** By forcing customers to return to Zenith Retail's own site to review bill details, the company achieves a strategic objective. Which of the following is the primary advantage derived from this specific setup?
(A) Reducing the pre-delivery float time to zero.
(B) Maintaining control over the customer experience to leverage targeted advertising and cross-selling.
(C) Allowing the consolidator to manage all customer interactions transparently.
(D) Converting all digital objects strictly into unstructured information.

**May/June 2024**

**115.** Once a call arrives at Apex Bank, it is instantly recognized and directed to the agent who is best suited to handle the specific financial query. Which telephony system enables this intelligent routing capability?

Click Here to Buy book on Amazon

# ANSWERS

1. (D) JEPI
The Joint Electronic Payment Initiative is a prominent technical standard sponsored by the World Wide Web Consortium to facilitate electronic business. This protocol allows websites to negotiate payment methods and providers automatically with the user's browser. It streamlines the transaction process by ensuring compatibility between various payment instruments and web-based merchant systems globally.

2. (C) Payments are directly connected to personal accounts instead of relying on a prepaid balance.
Real-time payment systems typically feature an open-loop architecture which ensures that transactions are linked directly to bank accounts rather than internal digital wallets. This approach provides faster settlement by bypassing the need for users to pre-fund a specific balance. Consequently, liquidity is maintained within the financial institution while allowing for instantaneous fund transfers.

3. (C) Financial-regulated payment services performed from or through a mobile device.
Mobile payment refers to financial services regulated by governing bodies that are executed using a mobile device. Instead of using cash, checks, or physical credit cards, consumers use their smartphones or tablets to pay for goods or services. This technology integrates telecommunications with financial systems to provide a convenient and efficient method for conducting commercial transactions.

4. (C) The MNO does the billing either on the prepaid user account or later on the phone bill.
In the mobile network operator-centric model, the operator manages the billing process for transactions. Purchases are charged either against the user's existing prepaid balance or added to their monthly postpaid cellular bill. This model leverages the established billing relationship between the operator and the customer, simplifying the payment process for digital goods and various small-scale services.

5. (B) Customer Relationship Management
Customer Relationship Management focuses on enhancing interaction by analyzing past behaviors to anticipate future needs. This concept utilizes customer self-service and personalized offerings to build long-term loyalty and satisfaction. By leveraging data-driven insights, organizations can tailor their products and services to individual preferences, ensuring a more relevant and engaging experience for every consumer within the business ecosystem.

6. (B) The billing company sends bill summary data to the consolidator while retaining bill detail information at their own Web site.
The hybrid model in electronic billing allows a billing company to send summary data to a third-party consolidator while keeping detailed information on its own server. This approach offers customers the convenience of viewing multiple summaries in one location. Simultaneously, it allows the billing company to maintain control over the customer relationship and leverage detailed viewing for marketing.

7. (B) It is the electronic sharing of structured or unstructured business information among suppliers, customers, and partners.
Electronic business involves the digital sharing of information across a broad network of suppliers, partners, and customers. It encompasses structured data exchange and unstructured communication to streamline organizational operations. This framework supports collaborative decision-making and operational efficiency by utilizing internet technologies to connect various stakeholders, thereby transforming traditional business processes into highly integrated and responsive digital value chains.

8. (B) It is be initiated by the customer using a mobile phone for obtaining information or performing a transaction.
A pull message in mobile banking is a request actively sent by a customer to obtain specific data or perform actions. For example, a user might text a code to receive their current account balance or

NODIA

(B) Issuer-Centric Billing
(C) Biller Direct Presentation
(D) Embedded Payments

**Oct/Nov 2012**

**122.** Read the following scenario and answer the questions that follow:
*FinNova, a rising FinTech firm, creates a complex global payment platform. When a customer pays, the platform dynamically connects multiple payment processors and gateways, utilizing AI to route the transaction through the fastest and cheapest pathway.*
Which emerging digital payment trend does this represent?
(A) Embedded Payments
(B) Buy Now, Pay Later (BNPL)
(C) Payment Orchestration
(D) Mobile Wallets

**May/June 2011**

**123.** FinNova launches an instant domestic transfer network that operates 24 x 7 x 365. Funds settle in seconds directly to personal accounts rather than being held in an intermediary wallet balance. Which characteristic of Real-Time Payments (RTP) does this direct connection to personal accounts describe?
(A) Post-paid Macro-Payment
(B) Pre-delivery float synchronization
(C) Open-loop architecture
(D) Closed-loop architecture

**Oct/Nov 2020**

**124.** FinNova introduces a new feature at checkout allowing consumers to split a large retail purchase into four equal monthly installments without any interest charge, generating an instant credit decision. Which payment model is FinNova leveraging?
(A) Buy Now, Pay Later (BNPL)
(B) White label financing
(C) Micro-Payments aggregation
(D) Open-loop Real-Time Payments

**May/June 2022**

**125.** To combat increasing e-commerce fraud, FinNova integrates a system that analyzes a consumer's unique swiping speed and phone-holding patterns to authenticate transactions silently. What specific security technology is FinNova deploying?
(A) One-Time Passwords (OTP)
(B) Behavioral Biometrics
(C) Computer Telephony Integration
(D) Screen Pops

www.nodia.in

Downloaded from www.pdf.tube

3. Company itself manages and controls the entire billing process
4. An on-line consolidation firm manages the process for the billing company

(A) P-3, Q-4, R-1, S-2
(B) P-1, Q-4, R-2, S-3
(C) P-4, Q-2, R-3, S-1
(D) P-3, Q-1, R-4, S-2

**May/June 2007**

**89.** Consider the following statements regarding the approach for E-banking:
1. Develop a sound business case to chart the e-business investment.
2. Review the internal process and security protocols in support of the E-business strategy.
3. Implement the chosen solution as a fully segregated unit independent of the core business.

Which combination of the statements is correct?
(A) 1, 2, and 3
(B) 1 and 2 only
(C) 2 and 3 only
(D) 1 and 3 only

**Oct/Nov 2025**

**90.** Identify the incorrect pair regarding Call Center Technologies.
(A) CTI - Automated Number Identification
(B) WFM - Forecasts the volume of customer interactions
(C) IVR - Natural language speech recognition
(D) ACD - Automatically dials from a list of phone numbers

**May/June 2012**

**91.** Each of the following questions consists of two statements, one labeled as Assertion (A) and the other as Reason (R). Select the correct answer from the options given below.
Assertion (A): The Self-owned inventory model provides better post-purchase customer experience and smoother operations.
Reason (R): The e-Commerce player owns the inventory, leading to ready information on location, supply chain, and effectively better control.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2014**

**92.** Apex Bank sets stringent performance goals for its newly established call center. Based on industry standard Call Center Benchmarks, what maximum limit should they target for their Abandonment Rates?
(A) Less than 1%
(B) Less than 2%
(C) Less than 5%
(D) Less than 10%

**May/June 2019**

**93.** Consider the following typical pull services in SMS banking:
1. Account balance enquiry
2. Mini statement request
3. Stop payment instruction on a cheque
4. Fixed deposit interest rates enquiry
5. Alert of insufficient funds

Which of the following accurately represents the combination of pull services?
(A) 1, 2, 4, and 5 only
(B) 1, 2, 3, and 4 only
(C) 2, 3, 4, and 5 only
(D) 1, 2, 3, 4, and 5

NODIA

**Oct/Nov 2006**

**94.** As Zenith Retail expands, they experience a surge in high volume, low-cost B2B supply transactions. To ensure seamless electronic business, which standardized protocol specifically designed for such high volume low-cost transactions should they adopt?
(A) OFX
(B) JEPI
(C) OBI
(D) OTP

**May/June 2021**

**95.** Each of the following questions consists of two statements, one labeled as Assertion (A) and the other as Reason (R). Select the correct answer from the options given below.
Assertion (A): Predictive dialers automatically dial from a list of phone numbers and detect busy signals, voicemail, and disconnected numbers.

a mini-statement. This interaction is customer-driven, providing on-demand access to financial information through their mobile device without requiring the bank to initiate contact.

**9.** (B) An e-commerce company sells its own brand goods through its website, typically earning higher margins.
The private label online business model involves an e-commerce firm selling products manufactured under its own brand name directly through its digital storefront. By controlling the branding and sourcing of these goods, companies can often achieve significantly higher profit margins compared to reselling third-party brands. This strategy also helps in building brand loyalty and differentiation in a competitive marketplace.

**10.** (C) NPCI
The National Payments Corporation of India functions as the authorized central unit for the Bharat Bill Payment System. It is responsible for setting business standards, rules, and procedures for bill payments across the country. By acting as the central clearing and settlement body, it ensures interoperability between different billers and payment service providers, facilitating a seamless payment experience.

**11.** (D) Security and online privacy emerged as the top two priorities for e-commerce customers, ahead of convenience.
Modern cybersecurity trends indicate a shift in consumer behavior where security and online privacy are now prioritized over convenience. As digital transactions increase, customers demand more robust protection for their personal and financial data. This trend drives financial institutions to invest in advanced authentication methods and privacy-enhancing technologies to maintain user trust and mitigate the risks of evolving cyber threats.

**12.** (C) An ordered sequence of bits with a unique identification representing a collection of operations and information.
Within electronic commerce building blocks, a digital object is defined as a specific sequence of bits identified uniquely. These objects encapsulate both data and the operations that can be performed on that data. They serve as the fundamental units for transactions, agreements, and digital assets, allowing for standardized handling, storage, and exchange across various computing platforms and network architectures.

**13.** (A) Connecting payment processors and gateways to provide a platform for enabling and optimizing payments.
Payment orchestration involves integrating various payment processors, gateways, and financial services into a single unified platform. This technology optimizes the transaction process by dynamically routing payments through the most efficient channels. It helps merchants reduce processing costs, improve success rates, and simplify the management of multiple payment methods across different regions, ultimately enhancing the overall checkout experience for consumers.

**14.** (C) Determining exchange terms, such as delivery, refund policies, and arranging for payment credit.
Negotiating in e-commerce involves the interactive process where buyers and sellers agree on the specific terms of a transaction. This includes establishing the final price, delivery schedules, and return or refund policies. It also covers the arrangements for payment credit and other contractual obligations. This stage is crucial for ensuring that both parties have a clear understanding of their responsibilities.

**15.** (D) It pools all customers on hold into a single waiting list, regardless of the contact channel.
Universal queuing is a call center strategy that merges incoming interactions from various channels into a unified waiting list. Whether a customer reaches out via phone, email, chat, or social media, they are placed in a single queue. This ensures that agents handle inquiries in a fair, chronological order and allows for more efficient management of workforce resources and response times.

**16.** (A) The exchange of goods or services between two or more parties using electronic tools and techniques to perform transactions.
Electronic commerce is the process of conducting business transactions through digital tools and networks. It involves the buying and selling of goods or services between parties via the internet or other electronic means. This encompass

Click Here to Buy book on Amazon

**67.** (A) 5, 2, 4, 1, 3
The chronological process for a consolidated bill begins with accessing the internet. Next, the user signs on to their email box. They then open the email announcing the new bill, select it to view the specific details, and finally click the payment hyperlink to approve the transaction. this sequence ensures a logical flow from notification to final payment execution.

**68.** (A) Both 1 and 2 are correct
Computer Telephony Integration uses screen pops to provide agents with immediate customer data, which is accurate. Similarly, an Automatic Call Distributor is a telephony system designed to recognize and route incoming calls to the most appropriate agent or terminal based on predefined rules. Both technologies are essential for modern call centers to improve efficiency and enhance the customer experience.

**69.** (B) 1 and 2 only
Mobile banking usually requires the specific account number of the payee, whereas mobile payments mask this information for privacy and security. However, the necessity of an account number is not identical for simple transactions; mobile payments are designed to be more convenient for low-value transfers like paying an auto fare. Thus, only the first two statements accurately describe the differences.

**70.** (A) P-3, Q-4, R-1, S-2
Predictive dialers automatically dial numbers and detect signals, while voice biometrics authenticates identity to prevent fraud. CRM servicing applications provide a 360-degree customer view and document all interactions. Campaign management systems are used in outbound call centers to provide agents with contact lists. These technologies work together to streamline call center operations and improve the quality of customer interactions.

**71.** (A) 1, 2, and 4 only
Real-time payments are characterized by near-instant initiation, clearing, and settlement, operating 24x7x365. They require banks to have always-on backend systems. However, they are not strictly defined by a closed-loop architecture; instead, they often use an open-loop model connected directly to bank accounts. This ensures that funds are moved quickly and securely between different financial institutions and personal accounts.

**72.** (A) P-2, Q-4, R-3, S-1
In marketplaces, sellers partner with platforms to manage stores. Self-owned inventory models involve the e-commerce player possessing the stock. Private labels feature a company's own branded goods competing with others. White labels involve a brand generating traffic while a third party manages the platform and services. These diverse models allow e-commerce companies to choose the best strategy for their operations.

**73.** (A) Both 1 and 2 are correct
Both statements regarding call center technology are correct. CTI utilizes screen pops to deliver customer information to agents as calls arrive, improving service speed. Simultaneously, ACD systems are responsible for the intelligent routing of incoming calls to the most suitable terminal or agent. These systems are foundational for efficient call center management and providing a personalized customer service experience.

**74.** (C) Mini-Payments - Between $2 and $20
Mini-payments are a category of transactions typically ranging between $2 and $20, targeting commonly purchased small retail items. This classification helps in determining the most efficient payment processing methods and fee structures. While micro-payments cover smaller amounts and macro-payments cover larger ones, mini-payments represent a significant portion of everyday digital commerce and retail transactions for consumers.

**75.** (A) 1, 2, and 3 only
Payments are categorized as micro-payments under $2, mini-payments between $2 and $20, and macro-payments over $20. However, the statement about prepayments decreasing costs as transaction numbers decrease is incorrect; usually, higher transaction volumes through prepayments help distribute fixed costs. Understanding these value-based categories is essential for developing appropriate payment systems and ensuring cost-effective processing for different transaction sizes.

NODIA

# STUDYING FROM PDFs?

# THINK AGAIN.

If you are studying only from PDFs,
you are wasting valuable time.

Research shows that learning from

**PRINTED BOOKS** has up to

**4× HIGHER RETENTION**

than studying from screens.

**PRINT BOOK = BETTER MEMORY**

**PDF = LOWER RETENTION**

Those who study from **PRINTED BOOKS**
move **AHEAD.**

Others are left **BEHIND**
in competition.

In competitive exams,
being average is not enough.

## STAY ONE STEP AHEAD.

Internet Mail Extensions allow for the exchange of various media types. These protocols form the technical foundation for seamless data sharing and e-business activities.

**25.** (B) It displays a customer's profile automatically using ANI or a front-end identification request.
Within Computer Telephony Integration, a screen pop is a feature that automatically displays a customer's data on an agent's monitor as a call connects. It uses Automatic Number Identification or other identifiers to retrieve the relevant profile from the database. This immediate access to customer history and information allows the agent to provide personalized service and resolve issues more quickly.

**26.** (D) A bank-initiated message sent to a customer's mobile phone without a prior request for that specific information.
A push message in SMS banking is a notification sent by a financial institution to a customer's mobile device without a specific request. These messages are often used for alerts, such as notifying the user of a large transaction, a low balance, or the availability of an e-statement. Push services help customers stay informed about their account activity in real-time.

**27.** (A) They are notifications about transactional activities delivered to the customer via SMS.
Banking alerts are automated notifications sent to customers via SMS to provide updates on their account or credit card activity. These alerts can include information about withdrawals, deposits, or reaching a credit limit. By providing real-time information, these alerts help customers monitor their finances more effectively and quickly identify any unauthorized or suspicious transactions on their accounts.

**28.** (C) 2000
The first patent specifically defining a "Mobile Payment System" was filed in the year 2000. This milestone marked the formal recognition of using mobile devices as a primary tool for executing financial transactions. Since then, the technology has evolved rapidly, moving from simple SMS-based systems to the sophisticated mobile wallets and contactless payment methods that are widely used today.

**29.** (C) Reducing the economic distance between producers and consumers.
A direct benefit of e-commerce is its ability to reduce the economic distance between producers and consumers. By eliminating intermediaries and physical storefront requirements, manufacturers can sell directly to their target audience. This streamlines the supply chain, often resulting in lower prices for customers and higher margins for producers. It also allows businesses to reach a global market more easily.

**30.** (D) A trusted third party operates as a neutral intermediary between financial agents and operators.
The Independent Service Provider model for mobile payments features a neutral third party that acts as an intermediary between financial institutions and mobile network operators. This provider manages the transaction flow and ensures that both the bank and the operator can interact securely. This model often facilitates interoperability across different networks and banks, providing a more flexible payment ecosystem.

**31.** (C) Cross-selling transforms the call center strictly into an absolute cost-center.
Cross-selling in call centers is a strategy aimed at offering additional products or services to existing customers during interactions. Contrary to being a cost-center, consistent cross-selling can transform a call center into a profit-generating unit. Agents use the opportunity of resolving issues to identify and fulfill further customer needs, thereby increasing revenue and strengthening the overall customer relationship.

**32.** (B) Acquirer-centric model
Online bill presentment and payment typically involve the biller direct model, the consolidator model, or a hybrid model. These frameworks determine how bills are presented and paid digitally. The acquirer-centric model is a mobile payment model rather than a standard electronic bill presentment and payment structure. Understanding these distinctions is essential for organizations choosing the right digital billing strategy for customers.

NODIA

**85.** (D) Both 1 and 2 are incorrect
The definitions for push and pull messages are swapped in the statements. A push message is initiated by the bank without a request, while a pull message is initiated by the customer to request information. Since the statements provide the opposite definitions, both are considered incorrect. Accurate terminology is essential for understanding how communication flows between banks and customers.

**86.** (C) P-2, Q-4, R-1, S-3
In e-commerce, ordering involves a contractual agreement on exchange terms. Billing involves sending remittance information to the buyer. Payment and settlement occur when the seller analyzes and accepts the remittance as valid. Distribution and receipt happen when the seller provides proof or delivers the goods. This sequence ensures that each stage of the digital transaction is completed and documented correctly.

**87.** (B) 1, 2, and 3 only
Starting e-commerce activities requires a hosting server, a network system, and a registered domain name. A purely manual order entry architecture is not a required component for e-commerce, as the goal is to automate the process through digital integration. These technological foundations allow businesses to establish an online presence and facilitate transactions with customers in a secure and efficient manner.

**88.** (A) P-3, Q-4, R-1, S-2
In the biller direct model, the company manages the entire process itself. The consolidator model uses a third party to manage the process for the company. The hybrid model sends summary data to a third party while keeping details on the company site. Pre-delivery float time is the period between data availability and customer receipt. These models define digital billing.

**89.** (B) 1 and 2 only
Successful e-banking implementation involves developing a sound business case and reviewing internal security protocols. However, it should not be implemented as a fully segregated unit; instead, it should complement and integrate with the core business. This ensures a unified brand experience and allows the organization to leverage its existing infrastructure and customer base while expanding into digital services.

**90.** (D) ACD - Automatically dials from a list of phone numbers
An Automatic Call Distributor is responsible for routing incoming calls, whereas a predictive dialer is the technology that automatically dials numbers from a list. The other pairs, such as CTI using ANI, WFM forecasting volumes, and IVR using speech recognition, are correctly matched. Understanding the specific function of each call center technology is essential for optimizing service and agent efficiency.

**91.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
The self-owned inventory model provides a better customer experience because the e-commerce company owns the stock and has direct control over the supply chain. This ownership ensures ready information on product location and availability, leading to smoother operations and more reliable delivery. The reason provided correctly explains why owning inventory results in a more efficient and effective post-purchase experience.

**92.** (B) Less than 2%
Industry standards for call centers recommend that abandonment rates should be kept to less than 2%. This target ensures that very few customers hang up before reaching an agent, reflecting a high level of accessibility and service quality. Monitoring this metric is crucial for organizations like Apex Bank to ensure they are meeting customer expectations and managing wait times effectively.

**93.** (B) 1, 2, 3, and 4 only
Pull services in SMS banking are initiated by the customer and include account balance enquiries, mini-statement requests, stop payment instructions, and interest rate enquiries. An alert for insufficient funds is a push service because it is initiated by the bank to notify the customer of an event. Correctly identifying pull services helps in understanding how customers interact with their banks.

Downloaded from www.pdf.tube

41. (A) 3, 4, 2, 1
Enabling e-commerce typically follows a logical sequence. First, a database-driven online catalogue is developed. Next, secure online ordering is provided by integrating the front-end with an order entry system. Then, static billing data is moved to an interactive web-based server. Finally, electronic payment methods are accepted to complete the full transaction or bill payment process for the customer.

42. (C) They remain valid indefinitely until the customer completes the transaction.
One-time passwords are secure codes used for authentication that expire after a very short period. They are not valid indefinitely, which is a key security feature to prevent unauthorized access if the code is intercepted. Sent via SMS, these passwords replace static credentials for individual transactions, significantly reducing the risk of cyber fraud in online and mobile banking environments.

43. (B) Number of Software Agents deployed
Standard call center benchmarks include abandonment rates, average speed of answer, and the number of calls handled per agent. These metrics help managers evaluate efficiency and service quality. The total number of software agents deployed is an operational count but is not considered a standardized performance benchmark used to measure the quality or speed of customer service interactions.

44. (D) Manual cheque truncation
Key activities in electronic commerce include advertising, shopping, negotiating, ordering, billing, and settlement. These processes are performed using digital tools to facilitate transactions. Manual cheque truncation, while a financial process, is not a core activity of e-commerce, which focuses on electronic data exchange and digital interaction to replace traditional manual and paper-based methods for buying and selling.

45. (C) To avoid the hefty card swipe fees levied by major credit card companies.
Merchants are incentivized to drive the shift toward mobile wallets primarily to reduce the costs associated with traditional credit card processing. Major credit card companies charge swipe fees for every transaction, which can significantly impact profit margins. Mobile wallets often utilize alternative payment rails or direct bank transfers that offer lower processing fees, providing a more cost-effective solution.

46. (B) The brand avoids taking responsibility for generating website traffic and providing services.
In a white label model, a branded online store is managed by an e-commerce player or a third party, but the brand itself typically takes responsibility for generating website traffic. This model helps build trust and customer loyalty while leveraging external technology for operations. It is incorrect to say the brand avoids traffic generation, as marketing and customer engagement are essential.

47. (B) The billing company retains full control over the bill detail data and customer interaction to leverage targeted advertising and cross-selling.
Combining the biller direct model with summary consolidators allows companies to retain control over detailed bill data and customer interactions. While the consolidator provides a summary for convenience, the customer must visit the biller's site for details. This ensures the billing company can use those visits for targeted advertising and cross-selling, maintaining a direct and valuable relationship.

48. (B) The billing company gains maximum opportunity to establish and maintain a personal, direct relationship with each customer.
The pure consolidator model manages the billing process on behalf of the company, which often results in the billing company losing the opportunity for a direct relationship. Since the customer interacts primarily with the consolidator's site, the biller has less control over the user experience and marketing. The main goal is providing one-stop-shopping convenience for the consumer.

49. (A) International Letters of Credit
The Bharat Bill Payment System supports various modern payment modes, including internet banking via NEFT, UPI, credit and debit cards, and Aadhaar-based payments. It is designed for domestic utility and service bill payments. International Letters of Credit are complex trade finance instruments and are not a supported

NODIA

**33.** (B) They inherently include the user profile's personal secrets and likes/dislikes.
Contracts as digital objects include instructions for handling, routing, and payment terms, but they do not inherently store a user's personal secrets or detailed behavioral likes and dislikes. Digital contracts are functional agreements that can be negotiated, signed, and exchanged electronically. While they interact with user profiles, their primary purpose is to define legal and operational terms for a transaction.

**34.** (D) It helps deliver the right products leading to repeat sales, and promotes the perception of a one-to-one personal relationship.
Personalization in electronic bill presentment and payment allows companies to deliver highly relevant content and product recommendations based on individual customer data. This targeted approach fosters a sense of a one-to-one relationship, which can significantly enhance customer loyalty. By presenting the right offers at the right time, businesses can drive repeat sales and improve the overall effectiveness.

**35.** (A) TDM (Time Division Multiplexing)
While OBI, JEPI, and OFX are established standards for electronic business and financial exchange, Time Division Multiplexing is a telecommunications technique for transmitting multiple signals over a single channel. TDM is related to how data is transported in telephony rather than being a specific functional standard for e-business transactions. E-business standards focus on negotiating payments and structured data exchange.

**36.** (A) Payments are directly connected to personal accounts instead of relying on a prepaid balance to accelerate the process.
The open-loop characteristic in real-time payments signifies that the transaction is linked directly to a customer's personal bank account. This eliminates the requirement for a separate prepaid balance or digital wallet to fund the payment. It ensures that funds are transferred immediately from the sender's account to the receiver's account, facilitating faster clearing and settlement within the banking system.

**37.** (A) Increase in order entry errors leading to extensive manual rework.
Supply Chain Management is designed to improve productivity and lower operating costs by reducing inventory and enhancing data integrity. It aims to reduce, rather than increase, order entry errors through automation and better communication. By streamlining processes, organizations can respond more quickly to market demands and improve their competitive position through more accurate and efficient logistics and procurement.

**38.** (D) Mega-Payments
Payments are categorized based on value into micro-payments for very small amounts, mini-payments for mid-range retail items, and macro-payments for larger transactions. Mega-payments is not a standard term used in this classification. Understanding these categories helps in choosing appropriate payment technologies and fee structures, as the processing requirements and security needs vary significantly depending on the transaction value.

**39.** (D) A reliable method to authenticate a person's identity based on unique vocal characteristics to prevent fraud.
Voice biometrics is a security technology used in call centers to verify a person's identity by analyzing their unique vocal patterns. Unlike passwords which can be forgotten or stolen, voice prints are difficult to replicate, providing a high level of security. This method helps prevent fraud during phone-based transactions and improves the customer experience by simplifying the authentication process.

**40.** (D) Customers must pay substantial interest charges on every installment regardless of the provider.
Buy Now, Pay Later products are often attractive to consumers because many providers offer interest-free installment options. While some versions may charge fees or interest, the general appeal is the ability to spread payments over time without the high costs associated with traditional credit cards. Credit decisions are typically made in minutes, providing a convenient alternative for modern shoppers.

Click Here to Buy book on Amazon

**58.** (A) Payments rely strictly on a closed-loop prepaid balance to accelerate the process.
Real-time payments are designed to clear and settle transactions in seconds, typically using an open-loop architecture connected directly to bank accounts. They do not rely strictly on closed-loop prepaid balances. These systems operate 24x7x365 and require banks to maintain backend systems that can process transactions at any time, ensuring that funds are available to recipients immediately.

**59.** (C) To pool all customers on hold into a single waiting list, regardless of the contact channel used.
The primary goal of universal queuing in a call center is to manage customer wait times more effectively by creating a single, unified queue for all channels. By pooling phone calls, emails, and chats, managers can ensure that the next available agent handles the longest-waiting customer regardless of how they contacted the company. This improves efficiency and service fairness.

**60.** (B) Treasury bills and bonds
Software agents in e-commerce include translators that handle data conversion, escrow agents that manage trusted transactions, and workflow managers that coordinate internal processes. Treasury bills and bonds are financial instruments and investments, not software agents used as building blocks for electronic commerce. Software agents are automated programs that perform specific tasks to facilitate digital business operations and information exchange.

**61.** (A) P-3, Q-1, R-4, S-2
In the acquirer-centric model, the merchant handles the mobile device interaction. The issuer-centric model may leave the merchant unaware of the mobile nature of the payment. The bank-centric model has the bank handling payments while the operator provides the connection. Finally, in the MNO-centric model, the network operator performs the billing on the prepaid account or phone bill.

**62.** (D) Both 1 and 2 are incorrect
The statements provided are incorrect because they swap the characteristics of the billing models. The biller direct model is what allows companies to tailor presentation and retain customer data. Conversely, the consolidator model is what provides customers with the convenience of viewing multiple bills in one location. Therefore, both descriptions fail to accurately represent their respective electronic billing frameworks.

**63.** (B) P-4, Q-2, R-3, S-1
E-business standards serve different roles: OBI is designed for high-volume, low-cost supply transactions. JEPI is a protocol sponsored by the World Wide Web Consortium. OFX is specifically tailored for financial institutions to exchange data. The OTP standard is used to facilitate transactions for purchasing customers. These standards ensure compatibility and security across various digital platforms and organizational systems.

**64.** (C) 1 and 3 only
The Bharat Bill Payment System is an interoperable bill payment system that supports multiple modes including UPI, cards, and net banking. While it is driven by the RBI, it was conceptualized by the National Payments Corporation of India, not IDRBT. Therefore, statements regarding its interoperability and payment modes are correct, but the conceptualization statement is inaccurate based on its history.

**65.** (B) OFX - For financial institutions
Open Financial Exchange is a standard designed specifically for financial institutions to exchange data electronically. It facilitates the flow of information between banks and their customers or other financial organizations. While other standards like JEPI and OBI exist for different e-business functions, OFX is the correct protocol for financial data exchange, supporting activities like bill payment and statement delivery.

**66.** (C) 1, 2, and 3 only
Industry benchmarks for call centers target abandonment rates under 2%, approximately 200 calls per agent daily, and an average speed of answer around 20 seconds. However, the percentage of blocked calls should be minimal, typically less than 1%, rather than over 10%. Maintaining these standards ensures efficient operations and high levels of customer satisfaction within a service environment.

NODIA

activities such as online retail, electronic data interchange, and digital payments, enabling organizations to reach broader markets and operate with increased speed and efficiency.

**17.** (A) Develop a sound business case to chart the e-business investment.
Implementing e-banking requires a strategic approach, beginning with the development of a sound business case to justify the investment. Organizations must evaluate the potential return on investment, market demand, and technological requirements. This foundational step ensures that the e-banking strategy aligns with the overall business goals and provides a clear roadmap for resource allocation and risk management.

**18.** (C) Less than 1%
Industry benchmarks for call center performance suggest that the percentage of blocked calls, where a caller receives a busy signal, should be kept extremely low. Maintaining a rate of less than 1% is a common target to ensure high customer accessibility. Minimizing blocked calls is essential for maintaining customer satisfaction and preventing users from seeking services from competitors due to unavailability.

**19.** (D) They allow non-finance or non-fintech merchants to accept payments within non-payment apps.
Embedded payments integrate financial transaction capabilities directly into non-financial applications or websites. This allows customers to complete purchases without being redirected to an external banking portal or payment site. For example, a ride-sharing app or a retail platform can process payments natively. This creates a frictionless user experience, reducing checkout abandonment and allowing merchants to capture more consumer data.

**20.** (A) Mobile payments mask the account number from the public, whereas mobile banking requires a known payee account number.
A fundamental difference between mobile banking and mobile payments is how the user identifies the recipient. Mobile banking typically requires the specific bank account number of the payee for fund transfers. In contrast, mobile payment systems often mask account details from the public, using tokens or unique identifiers like phone numbers. This enhances security and simplifies transactions in public settings or retail environments.

**21.** (C) Transactions can be initiated through multiple payment channels including POS, ATM, Bank Branch, and Agents.
Bharat BillPay is designed for maximum accessibility, allowing transactions to be initiated through a wide variety of channels. Customers can pay their bills at physical locations like bank branches, agent outlets, and point-of-sale terminals. Additionally, digital channels such as ATMs, internet banking, and mobile wallets are supported. This multi-channel approach ensures that bill payment services are available to both urban and rural populations.

**22.** (B) SCM, CRM, and E-commerce
E-business operates across three core dimensions: Supply Chain Management, Customer Relationship Management, and E-commerce. Supply chain management streamlines internal and partner processes, customer relationship management focuses on customer interactions and personalization, and e-commerce handles the actual online buying and selling transactions. Together, these elements form a comprehensive framework for modern digital business operations and organizational efficiency.

**23.** (D) Supply Chain Management
Supply Chain Management fundamentally deals with the coordination of procurement, forecasting, and logistics through digital tools like extranets and groupware. It focuses on streamlining the flow of goods and information from suppliers to the final consumer. By analyzing data and optimizing inventory levels, organizations can reduce costs and improve responsiveness, ensuring that products are delivered efficiently and effectively.

**24.** (D) FTP, HTTP, SMTP, and MIME
Digital object operations and information exchange rely on standardized protocols and APIs to ensure interoperability across networks. File Transfer Protocol handles file movements, Hypertext Transfer Protocol facilitates web communication, and Simple Mail Transfer Protocol manages email delivery. Multi-purpose

Downloaded from www.pdf.tube

**76.** (A) P-3, Q-1, R-4, S-2
Supply Chain Management streamlines internal processes, while Customer Relationship Management brings customers and associates closer together. E-commerce is used for online purchases, and groupware refers to email-integrated collaborative software. These four dimensions represent the core components of e-business, ensuring that internal operations, external sales, and customer interactions are all managed efficiently through digital technologies and platforms.

**77.** (B) 1 and 2 only
Chatbots use natural language processing to understand intent and can recognize multiple languages. While they are a form of conversational AI, they do not completely replace traditional IVR systems; rather, they often complement them to provide more advanced self-service options. Together, they allow organizations to handle high volumes of inquiries and provide customers with faster, automated responses.

**78.** (A) P-3, Q-4, R-1, S-2
CTI enables computer-telephone interaction with screen pops. ACD recognizes and routes incoming calls to the best-suited agent. Intelligent callback allows callers to be contacted later instead of waiting, and universal queuing pools all customers from different channels into a single waiting list. These technologies are vital for modern call centers to optimize resource allocation and improve customer satisfaction.

**79.** (A) Both 1 and 2 are correct
Buy Now, Pay Later technologies grew significantly during the pandemic as a credit card alternative. Payment orchestration also simplifies global payments by using real-time analytics and intelligent routing. Both statements are correct, reflecting key trends in the evolving digital payment landscape. These innovations help businesses reach more customers and manage complex transaction flows more efficiently and cost-effectively.

**80.** (A) Bounced cheque - Credit Card Related Alert
A bounced cheque is a banking-related alert, not a credit card alert, as it pertains to a traditional bank account transaction. Credit card alerts typically involve reaching credit limits or reminders for due dates. Banking alerts often cover ATM withdrawals and account-specific events. Correctly categorizing these notifications ensures that customers receive relevant and accurate information regarding their financial activities.

**81.** (B) 2 and 3 only
Electronic billing systems reduce value lost during pre-delivery float time and enable sophisticated personalization with targeted messages. They do not require high investment in printing, as they are digital, and they move customers toward lower-cost digital channels rather than higher-cost paper ones. By utilizing customer data, these systems provide a more efficient and engaging way to manage billing and payments.

NODIA

**82.** (A) P-2, Q-4, R-1, S-3
Unstructured information includes freeform text and media like voice or video. Structured information consists of organized data like EDI messages or electronic forms. Objects for sale are items like software and movies. Agents and brokers act as information filters or trusted third parties. This classification helps in managing the different types of digital content and services.

**83.** (A) P-3, Q-2, R-4, S-1
Buy Now, Pay Later allows customers to spread payments over time. Mobile wallets use smartphone apps for contactless payments. Payment orchestration connects multiple processors into one platform. Real-time payments utilize an open-loop model connected directly to personal bank accounts. These trends represent the primary innovations driving the growth and efficiency of the modern digital payment ecosystem for consumers and merchants.

**84.** (C) 1, 2, and 3
SMS banking inherently lacks encryption, which is a significant security concern. However, banks have introduced compensating controls like security tokens and pre-registration for high-risk transactions to mitigate these risks. These methods allow financial institutions to offer the convenience of SMS banking while maintaining a necessary level of security, ensuring that sensitive customer data and transactions remain protected.

payment mode within the BBPS framework, which focuses on consumer bill payments.

**50.** (C) Logistics-centric model
Primary models for mobile payments include the bank-centric model, where the bank handles transactions, and the operator-centric model, where the mobile network operator manages billing. The independent service provider model uses a neutral third party. Logistics-centric is not a recognized primary model for mobile payments, as it focuses on the movement of goods rather than the processing of financial transactions.

**51.** (D) They deliver a frictionless purchase journey by allowing merchants to accept payments natively within non-payment apps.
Embedded payments significantly improve the user experience by providing a frictionless purchase journey. By allowing merchants to accept payments natively within their own applications, they eliminate the need for users to navigate away to external banking portals. This streamlined process reduces checkout time and abandonment rates, making it easier for customers to complete transactions within their preferred apps.

**52.** (D) TDM has largely replaced IP as the primary mechanism for transporting call center transactions.
In call centers, Internet Protocol has largely replaced traditional Time Division Multiplexing because it offers more flexibility and lower costs. IP networks allow for integrated services like instant messaging and video calling alongside voice. TDM is an older technology that segments signals, while IP enables phone calls to be made directly from websites and through more efficient data networks.

**53.** (C) Restrict electronic payment methods exclusively to offline cheque clearing.
To enable e-commerce, organizations must develop digital catalogues, move billing data to interactive servers, and provide secure online ordering. Restricting payment methods to offline cheque clearing is contrary to the goals of e-commerce, which seeks to facilitate instant digital transactions. Successful e-commerce requires the integration of electronic payment methods like cards or digital wallets to ensure a seamless process.

**54.** (C) Customers expect a consistent, personalized, and relevant experience regardless of the channel they interact through.
Organizations prioritize omnichannel support because modern customers expect a consistent and personalized experience across all interaction points. Whether they use phone, chat, email, or social media, the quality and relevance of the support should remain high. Omnichannel strategies ensure that customer data and history are shared across channels, allowing for more effective and efficient resolution of issues.

**55.** (A) Foreign currency exchange rates enquiry
Periodic account balance reports, e-statement notifications, and alerts about cleared cheques are examples of push services initiated by the bank. A foreign currency exchange rate enquiry is typically a pull service because it is initiated by the customer when they need specific information. Push services are designed to keep the customer updated on account status without requiring a request.

**56.** (A) The customer and his agent are exclusively in charge of handling the interaction with the mobile device.
In the acquirer-centric mobile payment model, the merchant and their agent are responsible for handling interactions with the mobile device. This is often contrasted with issuer-centric models. It is incorrect to say the customer and their agent are exclusively in charge, as this model focuses on the merchant's role in facilitating the payment transaction at the point of sale.

**57.** (A) They provide credit decisions in minutes, are easier to obtain than traditional credit, and offer manageable installment options often at no interest.
The core advantage of Buy Now, Pay Later products is their accessibility and convenience. Consumers can receive credit decisions almost instantly, and the requirements are often less stringent than traditional credit cards. The ability to pay in manageable installments, frequently without interest, makes these products highly appealing for retail purchases, especially among younger consumers who prefer flexible financing.

Click Here to Buy book on Amazon

**94.** (C) OBI
Open Buying on the Internet is a standard specifically designed for high-volume, low-cost B2B supply transactions. It provides a framework for secure and efficient electronic procurement between organizations. By adopting OBI, Zenith Retail can streamline its supply chain interactions, ensuring that frequent and low-value business transactions are handled with minimal manual intervention and maximum technological compatibility across different systems.

**95.** (C) Assertion (A) is true, but Reason (R) is false.
Predictive dialers are designed to automate the dialing process and detect busy signals or voicemail, which increases agent efficiency. Therefore, the assertion is true. However, the reason is false because these systems are built to eliminate the need for agents to manually listen to every dialing sequence, allowing them to focus only on calls that have successfully connected to a person.

**96.** (B) Pull service
This interaction is a pull service because the customer initiated the request for specific information, such as current exchange rates. The bank's response is provided only after receiving the user's SMS. Pull services empower customers to access banking information on-demand, providing a convenient way to manage financial needs while traveling without needing to contact a live representative.

**97.** (D) 1, 2, 3, 4, and 5
Electronic commerce involves a comprehensive set of key activities: advertising and shopping, negotiating terms, ordering goods, billing, and the final payment and settlement. All five activities are essential components of the digital transaction lifecycle. Together, they form a structured process that allows buyers and sellers to interact, agree on terms, and complete commercial exchanges using electronic tools and networks.

**98.** (A) Automated Number Identification (ANI)
Automated Number Identification is the specific feature of Computer Telephony Integration that identifies the caller's telephone number. It allows the system to instantly recognize the customer and retrieve their profile from the database before the agent even answers the call. This technology is vital for providing personalized service and reducing the time required for customer identification during a support interaction.

**99.** (B) Hybrid model
Zenith Retail is using the hybrid model because it sends summary data to a third-party portal while requiring customers to visit its own site for detailed bill information. This model balances the convenience of a consolidator for initial notification with the biller's need to maintain control over the detailed customer experience and leverage opportunities for targeted communication and marketing.

**100.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
In mobile payment architectures, the account number is masked from the public, which allows users to transfer money without knowing the recipient's specific bank details. This enhanced privacy is a core feature of mobile payments, making them simpler and more secure for public transactions. The reason correctly explains why knowing the account number is unnecessary in this modern payment framework.

**101.** (A) The total absenteeism and masking of the bank account number in mobile payments.
This scenario highlights the concept of account number masking, which is a key difference between mobile payments and traditional mobile banking. In mobile payment systems, unique identifiers like phone numbers or tokens are used instead of bank account numbers. this absenteeism of the account number from the public view enhances security and makes peer-to-peer transfers more convenient in social settings.

**102.** (C) 1, 2, 3, and 4 only
CTI, IVR, WFM, and QM are all recognized and essential technologies used in modern call centers to manage interactions, automate responses, and ensure quality. Electromagnetic Pulse Mitigation is a specialized defense or infrastructure technology and is not a standard call center application. Understanding these core technologies helps organizations optimize their

Downloaded from www.pdf.tube

Section 66, while defamatory emails fall under 67.
(C) Sending obscene emails carries a maximum fine of Rs. 1 crore under Section 43 of the IT Act.
(D) Threatening emails are exclusively penalized by the Supreme Court in a direct proceeding.

**Oct/Nov 2005**

**25.** How does Section 72 of the IT Act conceptually protect users?
(A) By mandating DRM for all private digital communications.
(B) By penalizing the breach of confidentiality and privacy with fines and imprisonment.
(C) By requiring banks to issue public key pairs to all account holders.
(D) By allowing the government to intercept protected systems without restrictions.

**May/June 2020**

**26.** Under the scope of Data Theft, which of the following is explicitly included as an object of theft?
(A) Only confidential customer information.
(B) Hardware peripherals and storage devices.
(C) Digitally printed ledger books.
(D) Source or object code.

**Oct/Nov 2015**

**27.** Which statement is correct regarding the Controller's authority to issue orders under Section 68 of the Information Technology Act?
(A) Anyone who fails to comply will be sentenced to three years in jail and a fine.
(B) Failure to comply with any orders results in a life sentence.
(C) The Controller can only issue orders regarding foreign nationals.
(D) The orders can be freely ignored if they contradict DRM metadata.

**May/June 2023**

**28.** When were the Information and Technology (IT) Rules, 2021 framed by the Union Government?
(A) February 25
(B) March 24
(C) January 1
(D) April 15

**Oct/Nov 2021**

**29.** Which statement is correct regarding the retention of electronic records under the Information Technology Act?
(A) The record must be retained in an entirely different format to ensure security.
(B) Details identifying the origin and destination can be omitted if the record is encrypted.
(C) Information must remain accessible so as to be usable for subsequent reference.
(D) Electronic records can only be retained for a maximum period of 5 years.

**May/June 2024**

**30.** Conceptually, what constitutes a computer crime regarding misrepresentation to the Controller or Certifying Authority?
(A) Submitting a digitally signed document that contains minor typographical errors.
(B) Using a digital signature on multiple distinct and authorized e-banking portals.
(C) Retaining electronic records beyond the statutory time frame for public access.
(D) Suppressing material facts or making misrepresentations to obtain a certificate.

**Oct/Nov 2008**

**31.** Which of the following was NOT introduced by the Information Technology (Amendment) Act, 2008?
(A) Section 66A penalizing offensive messages.
(B) Section 69 regarding interception or monitoring of information.
(C) The foundational legal recognition of Digital Signatures.
(D) Penalties for cyber terrorism and voyeurism.

**May/June 2006**

**32.** Which of the following documents is NOT among the exempted documents from the applicability of the IT Act?
(A) A document executing a Negotiable Instrument under the Negotiable Instruments Act, 1881.
(B) Power of execution of an attorney.
(C) Application form for opening a bank account electronically.
(D) A contract for the sale of immovable property.

NODIA

mobile device. This mechanism replaces static passwords, which are more vulnerable to theft, and is a standard tool for combating fraud in digital banking.

**112.** (D) Assertion (A) is false, but Reason (R) is true.
The assertion is false because e-business is much more than just a destination; it is a fundamental transformation of business processes and communications. However, the reason is true as e-business is indeed drastically changing how we live and work today. E-business encompasses a wide range of activities beyond simple digital marketplaces, including supply chain management and information sharing.

**113.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
The RBI has made SMS alerts mandatory for certain transactions, such as cheque clearing, to help combat the rise in fraud. By notifying customers in real-time about cheque activity, they can quickly identify and report unauthorized transactions. The reason provided correctly explains the regulatory motivation behind this mandate, which is aimed at protecting consumers and ensuring the integrity of the banking.

**114.** (B) Maintaining control over the customer experience to leverage targeted advertising and cross-selling.
By requiring customers to visit their own site to view bill details, a company maintains control over the customer experience. This allows them to use the interaction for targeted advertising and cross-selling other products. This strategy ensures that the company does not lose the opportunity to engage with its customers directly, even when using third-party consolidators for initial bill summaries.

**115.** (D) Automatic Call Distributor (ACD)
An Automatic Call Distributor is the telephony system responsible for recognizing and directing incoming calls to the most suitable agent. It uses predefined rules, such as agent skill level or availability, to ensure that the customer is connected to someone who can best handle their query. This intelligent routing is essential for optimizing call center efficiency and providing a high quality service.

**116.** (A) 1, 2, 3, and 5 only
Contracts as digital objects include instructions for handling, can be negotiated and amended, and can be bought or sold. However, electronic cash is specifically designed to be difficult to alter, reproduce, or copy to prevent fraud. Therefore, statement 4 is incorrect, while the other features accurately describe how digital contracts function as versatile building blocks in electronic commerce and business agreements.

**117.** (D) MNO-centric model
This scenario represents the MNO-centric model because the mobile network operator is responsible for billing the transaction directly to the user's phone bill. In this model, the operator leverages its existing billing relationship with the customer to facilitate payments for digital goods. The bank's role is minimized, as the financial settlement occurs through the telecommunications company's own accounting and billing.

**118.** (D) Assertion (A) is false, but Reason (R) is true.
The assertion is false because banks have not completely abandoned SMS banking; rather, many continue to use it by implementing compensating controls to mitigate the lack of encryption. The reason is true as these controls, such as limiting transaction values or using security tokens, allow banks to provide a convenient service while managing the inherent risks associated with the SMS channel.

**119.** (A) Private label
Zenith Retail is employing the private label model by manufacturing and selling its own branded goods directly through its website. This strategy allows the company to secure higher profit margins and build brand equity by offering exclusive products. It differentiates the company from competitors who only resell third-party brands and helps in creating a unique and loyal customer base.

**120.** (D) Assertion (A) is false, but Reason (R) is true.
The assertion is false because real-time payments do not rely strictly on prepaid balances; instead, they often use an open-loop model connected directly to bank accounts. The reason is true, as this open-loop characteristic is what allows for immediate fund transfers from personal

Click Here to Buy book on Amazon

customer service operations and improve overall agent performance and satisfaction.

**103.** (B) Workforce Management Software (WFM)
Workforce Management software provides the forecasting capabilities needed to predict future call volumes based on historical data. By analyzing past interaction patterns, it helps managers determine the optimal number of agents to schedule for different shifts. This ensures that staffing levels match demand, which is crucial for maintaining low wait times and providing efficient customer service in a call center.

**104.** (D) Assertion (A) is false, but Reason (R) is true.
The assertion is false because the pure consolidator model actually reduces the direct relationship between the biller and the customer by placing a third party in between. However, the reason is true; in this model, a customer's bill is often reduced to a single line on a consolidated page. This makes the model convenient for consumers but less effective for biller-led marketing.

**105.** (C) Push message
This automated alert is a push message because it is initiated by the bank to notify the customer of a specific event—in this case, a large withdrawal. The customer receives the notification without having to request it. Push messages are essential for real-time security monitoring and keeping customers informed about significant account activities, helping to quickly identify potential unauthorized transactions.

**106.** (A) 1, 2, 3, and 5 only
Periodic balance reports, withdrawal alerts, OTPs, and e-statement notifications are all push services because they are initiated by the bank to provide information or authentication. A foreign currency exchange rate enquiry is typically a pull service because it is requested by the customer. Identifying these distinctions is important for understanding the different ways banks communicate with their customers via SMS.

**107.** (A) White label
This scenario represents a white label model because Zenith Retail provides the brand name, while a third party handles the platform management, traffic generation, and payment gateway. This allows a company to offer a branded online store without having to build and manage the underlying technology infrastructure themselves. It leverages external expertise while maintaining brand identity and building customer trust.

**108.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Digital objects are easily created and modified because they are defined as a specific sequence of bits that can be accessed independently of any particular application. This application-independence is the reason why they can be reused and handled efficiently across different systems. The reason provided accurately explains the technical foundation that allows digital objects to be so versatile in e-commerce.

**109.** (D) Quality Management (QM)
Quality Management applications are used by call center managers to monitor agent performance and ensure adherence to internal policies, including scheduled breaks. By identifying areas of weakness and documenting interactions, QM tools help maintain high service standards and consistent operations. This software is essential for tracking how well agents follow protocols and for providing data-driven feedback to improve overall performance.

**110.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
The rapid rise in e-commerce and non-cash payments has led to an increase in cyber threats, which is the primary reason why payment providers are investing heavily in new cybersecurity solutions. Technologies like behavioral biometrics are being deployed to provide more robust protection against fraud. The reason correctly identifies the market conditions that are driving the need for advanced security measures.

**111.** (D) One-Time Password (OTP)
A secure, short-lived code sent via SMS is called a One-Time Password. It is used to provide an additional layer of security for high-value transactions by ensuring that the person completing the transfer has access to the registered

NODIA

# CHAPTER 13

# IT Act 2000 - 2008

Oct/Nov 2022

**1.** What is the prescribed punishment for tampering with computer source documents under Section 65 of the Information Technology (IT) Act?

(A) Up to 5 years in prison and a fine of up to Rs. 1 lakh.

(B) Up to 2 years in prison and a fine of up to Rs. 1 lakh.

(C) Up to 10 years in prison and a fine of up to Rs. 2 lakh.

(D) Up to 3 years in prison, a fine of up to Rs. 2 lakh, or both.

May/June 2013

**2.** What is the core conceptual mandate introduced by the IT Rules, 2021 for digital platforms?

(A) The absolute prohibition of peer-to-peer file exchange programs.

(B) The mandatory embedding of digital watermarks on all user content.

(C) The requirement for digital platforms to have grievance procedures.

(D) The automatic decryption of all encrypted messages on social media.

Oct/Nov 2018

**3.** How is a "Computer Virus" defined in the context of computer crimes?

(A) A script that generates digital signatures for unauthorized network access.

(B) An encrypted communication protocol utilized by advanced hacking collectives.

(C) Instructions or programs that degrade computer performance or attach to other resources.

(D) A set of instructions used solely for bypassing firewalls in protected systems.

May/June 2007

**4.** Which statement is correct regarding the introduction of a computer virus or contaminant?

(A) It is solely punishable by imprisonment of 10 years under Section 70.

(B) Section 66A governs the introduction of all malicious codes following the 2008 amendment.

(C) Compensation is provided under Section 43, and Section 66 applies if data loss occurs.

(D) Only the creator of the virus, not the introducer, is liable for damages and fines.

Oct/Nov 2025

**5.** If an originator has not agreed with the addressee on a particular method for acknowledgement of receipt of an electronic record, how may the acknowledgement be given?

(A) It must strictly be given through a digitally signed and encrypted return email.

(B) It can be given by any conduct sufficient to indicate the record was received.

(C) It must be acknowledged through a physical paper receipt sent via certified mail.

(D) Acknowledgement in such cases is legally void and the record must be sent again.

May/June 2012

**6.** Which statement is correct regarding Secure Distribution mechanisms in Digital Rights Management (DRM)?

(A) They completely eliminate the need for copyright laws.

(B) They generally use Encryption and Digital Watermarks.

(C) They are applied only to physical media such as printed books.

(D) They prevent the decryption of data even by authorized users with valid license rights.

Oct/Nov 2014

**7.** What defines an electronic record that is treated as valid according to the legal recognition granted under the Information Technology (IT) Act?

(A) Digital files stored on magnetic disks that maintain high accessibility levels.

(B) Accessible electronic records usable for subsequent reference.

(C) Printed computer outputs verified and

Downloaded from www.pdf.tube

stamped by a certified gazetted officer.
(D) Encrypted datasets requiring official decryption keys from a Certifying Authority.

**May/June 2019**

**8.** Conceptually, what does the offence of hacking entail under Section 66 of the IT Act?
(A) Data theft punishable exclusively by a financial fine without prison time.
(B) Unauthorized alteration of data punishable by imprisonment, fine, or both.
(C) Offences strictly governed by the Indian Evidence Act rather than the IT Act.
(D) Violations that restrict punishment to the confiscation of hardware systems.

**Oct/Nov 2006**

**9.** Which of the following statements is correct regarding the Certifying Authority's power to issue a Digital Signature Certificate?
(A) The Certifying Authority can grant the certificate without verifying if the applicant holds the private key.
(B) The reasons for rejecting an application for a Digital Signature Certificate must be recorded in writing.
(C) Digital Signature Certificates are only issued for transactions under the Negotiable Instruments Act.
(D) The Central Government directly issues all Digital Signature Certificates.

**May/June 2021**

**10.** On which date did the Supreme Court of India give the verdict that Section 66A of the IT Act 2000 is unconstitutional in its entirety?
(A) 25 February 2021
(B) 24 March 2008
(C) 24 March 2015
(D) 15 August 2012

**Oct/Nov 2010**

**11.** Which statement correctly describes the objective achieved by the Information Technology (IT) Act regarding transactions?
(A) It mandates paper-based communication for all banking transactions.
(B) It outlaws the use of digital portals for entering into commercial contracts.
(C) It removes all penal provisions from the Indian Evidence Act.
(D) It recognizes electronic data interchange and filing as legally valid means.

**May/June 2005**

**12.** What is the fundamental definition of Digital Rights Management (DRM)?
(A) A global treaty governing the distribution of pirated software.
(B) A cryptographic standard for securing all local online bank accounts.
(C) Systems protecting digital media from unauthorized redistribution.
(D) An electronic acknowledgement system for the receipt of digital forms.

NODIA

**Oct/Nov 2023**

**13.** What is the fundamental mechanism through which Digital Rights Management (DRM) controls the exploitation of digital content?
(A) By meta tagging content with relevant usage rules prior to the content being encrypted.
(B) By rewriting the source code of the host computer's operating system.
(C) By registering the content directly with the World Intellectual Property Organization.
(D) By completely disabling the user's internet connection upon unauthorized access.

**May/June 2018**

**14.** How does the submission of forms by electronic means conceptually facilitate e-banking?
(A) It requires customers to visit branches to sign physical copies of electronic forms.
(B) It mandates that banks must charge a premium fee for electronic form processing.
(C) It allows electronic account opening, removing the need for physical submission.
(D) It limits the submission of documents to those possessing a physical key pair.

**Oct/Nov 2016**

**15.** Which statement correctly identifies an introduction made by the Information Technology (Amendment) Act in 2008?
(A) It introduced the primary framework for the legal recognition of electronic records.
(B) It repealed the rules regarding the retention of physical banking ledgers.
(C) It removed the concept of extraterritorial jurisdiction.
(D) It introduced Section 66A which penalized "offensive messages".

May/June 2014

**16.** Which of the following best defines a "Computer Contaminant" according to the Information Technology Act?
(A) Instructions designed to damage, destroy, or usurp computer operations.
(B) Unauthorized access attempts resulting in physical degradation of local networks.
(C) Hardware devices attached to terminals to intercept data transmissions.
(D) Software specifically engineered to bypass Digital Rights Management protections.

Oct/Nov 2007

**17.** Which statement is correct regarding the court's power in case of verification of a digital signature?
(A) The court cannot direct the Controller to produce the Digital Signature Certificate.
(B) Verification is strictly limited to forensic laboratories without the involvement of the person affixing the signature.
(C) The Indian Evidence Act prohibits courts from verifying digital signatures on electronic records.
(D) The court may direct any other person to apply the public key listed in the certificate and verify the digital signature.

May/June 2025

**18.** Under Section 67 of the IT Act, what is the recommended punishment in the event of a second or subsequent conviction for sending pornographic or obscene emails?
(A) Imprisonment up to 10 years and fine up to Rs. 2 lakh.
(B) Imprisonment up to 5 years and fine up to Rs. 1 lakh.
(C) Imprisonment up to 3 years and fine up to Rs. 2 lakh.
(D) Compensation up to Rs. 1 crore.

Oct/Nov 2019

**19.** Conceptually, what served as the foundational basis for enacting the Information Technology Act 2000 in India?
(A) The World Intellectual Property Organization Copyright Treaty.
(B) The Indian Penal Code, 1860.
(C) The Bankers' Books Evidence Act, 1891.
(D) The United Nations' model law.

May/June 2009

**20.** Under which provision are emails that are defamatory in nature punishable?
(A) Section 500 of the Indian Penal Code (IPC).
(B) Section 66 of the IT Act.
(C) Section 67 of the IT Act.
(D) Section 43 of the IT Act.

Oct/Nov 2011

**21.** Which statement is correct regarding the compliance requirements for large digital platforms under the Information Technology (IT) Rules, 2021?
(A) Platforms with more than 5 million users must produce weekly compliance reports for the ministry.
(B) The rules apply exclusively to foreign digital portals operating without a registered Indian office.
(C) Large platforms must produce monthly reports on complaints received and actions taken.
(D) Compliance reports are submitted directly to the Supreme Court of India for judicial review.

May/June 2010

**22.** What was the exact structure of the original Information Technology (IT) Act?
(A) 15 sections, 4 chapters, and 13 schedules.
(B) 94 sections, 13 chapters, and 4 schedules.
(C) 104 sections, 10 chapters, and 2 schedules.
(D) 94 sections, 15 chapters, and 4 schedules.

Oct/Nov 2024

**23.** Which of the following best explains the conceptual requirement for the legal recognition of a digital signature?
(A) The signature must be verified by a gazetted officer before electronic transmission.
(B) The signature is only legally recognized if stored on a physical floppy disk device.
(C) Digital signatures are legally valid only for transactions exceeding Rs. 1 lakh.
(D) Signatures are recognized if authenticated by means prescribed by the government.

May/June 2017

**24.** Which of the following statements correctly differentiates between types of email abuse?
(A) Defamatory emails are under IPC 500, while threats fall under IPC intimidation.
(B) Pornographic emails are punishable under

Click Here to Buy book on Amazon

accounts. This architecture ensures that funds are moved quickly and efficiently without the need for intermediary balances.

**121.** (D) Embedded Payments
Allowing a customer to finalize a payment seamlessly within a non-financial app's own checkout page is a clear example of embedded payments. This technology integrates financial transaction capabilities directly into the merchant's application, creating a frictionless user experience. It eliminates the need for redirection to external sites, which helps reduce checkout abandonment and allows the merchant to maintain control over the.

**122.** (C) Payment Orchestration
This scenario represents payment orchestration, where a platform connects multiple processors and gateways to optimize the transaction flow. By using AI to route payments through the most efficient and cost-effective pathways, the platform improves success rates and reduces costs. Payment orchestration is an emerging trend that helps businesses manage complex global payment ecosystems through a single, unified integration and interface.

**123.** (C) Open-loop architecture
The direct connection to personal accounts for fund settlement is a characteristic of an open-loop architecture in real-time payments. Unlike closed-loop systems that require a specific prepaid balance or wallet, open-loop systems are linked directly to the banking network. This allows for instantaneous fund transfers between different financial institutions, ensuring that money is moved quickly and securely from the sender to the.

**124.** (A) Buy Now, Pay Later (BNPL)
Offering a feature that allows consumers to split a large purchase into interest-free installments with an instant credit decision is the definition of the Buy Now, Pay Later model. This payment option provides consumers with a flexible way to manage their finances at the point of sale. BNPL products have become highly popular due to their convenience, speed, and affordability.

NODIA

**125.** (B) Behavioral Biometrics
Behavioral biometrics is the technology used to authenticate users by analyzing their unique patterns of interaction, such as swiping speed and phone-holding angles. This silent authentication method provides a continuous layer of security that is difficult for fraudsters to mimic. It helps combat fraud in e-commerce by verifying that the person using the device is the authorized owner based on behavior.

Oct/Nov 2017

**33.** Which statement incorrectly interprets the amendment to the Banker's Book of Evidence Act, 1891?
(A) The definition of 'Banker's Book' now includes ledgers and cash books maintained in an electronic form.
(B) Banks are strictly required to maintain physical forms of all data alongside electronic forms.
(C) Data stored in a floppy, disc, or tape is adequate in a computerized environment.
(D) A certified copy of a printout from an electromagnetic storage device is recognized.

May/June 2008

**34.** In the context of computer crime, what does "Denial of Service (DoS)" most appropriately refer to under the Information Technology (IT) Act?
(A) Actions that deny access to any person authorized to use a computer network.
(B) A customer's refusal to pay electronic banking fees.
(C) The rejection of a digital signature certificate application by the Certifying Authority.
(D) The failure of an OTT platform to publish a monthly compliance report.

Oct/Nov 2013

**35.** Which of the following does NOT grant any person the right to insist that an organization must accept or issue documents in electronic form?
(A) The disclaimer stating that IT Act provisions do not confer rights to insist on electronic monetary payments.
(B) Legal Recognition of Electronic Records.
(C) Retention of Electronic Records.
(D) Acknowledgement of Receipt.

May/June 2015

**36.** What is the most appropriate description of Digital Rights Management's (DRM) primary goal compared to traditional copyright laws?
(A) To make content theft technically impossible rather than relying on legal actions after the fact.
(B) To prosecute offenders under the IPC after a copyright breach occurs.
(C) To ensure digital portals publish grievance redressal procedures.
(D) To enable seamless peer-to-peer file exchange of commercially marketed material.

Oct/Nov 2012

**37.** Which of the following statements regarding the acknowledgement of receipt of electronic records is incorrect?
(A) Without an agreed method, a record is deemed undelivered regardless of conduct.
(B) If the originator requests it, the receipt of the electronic record shall be acknowledged.
(C) Acknowledgement may be given by any communication or conduct sufficient to indicate receipt.
(D) The originator can stipulate that acknowledgement must be in a particular form.

May/June 2011

**38.** Which of the following is NOT among the salient offenses listed under the Information Technology (IT) Act 2000?
(A) Tampering with computer source documents.
(B) Misrepresentation to the Controller.
(C) Securing unauthorized access to a protected system.
(D) Breaching Indian Trust Act rules through electronic contract creation.

Oct/Nov 2020

**39.** In the new environment of e-business, what is the most appropriate primary role that Banks may play regarding Digital Signatures?
(A) Serving strictly as a repository for confiscated computer systems.
(B) Acting as a Certifying Authority.
(C) Developing DRM ripping software.
(D) Regulating the OTT platforms' grievance procedures.

May/June 2022

**40.** Which of the following Acts is incorrectly stated as being amended by the Information Technology (IT) Act?
(A) Indian Penal Code
(B) Indian Evidence Act
(C) Bankers' Books Evidence Act
(D) Negotiable Instruments Act

NODIA

May/June 2016

**41.** Arrange the following Acts in the chronological order of their original enactment:
I Information Technology Act
II Indian Penal Code
III Bankers' Books Evidence Act
IV Indian Evidence Act
(A) (IV), (II), (III), (I)
(B) (II), (IV), (III), (I)
(C) (II), (III), (IV), (I)
(D) (III), (II), (IV), (I)

Oct/Nov 2009

**42.** Which statement regarding Section 70 (Protected System) of the IT Act is incorrect?
(A) It deals with systems that the government declares as protected.
(B) Securing unauthorized access to a protected system is subject to imprisonment and a fine.
(C) The penalty under this section is strictly limited to financial compensation up to Rs. 1 crore.
(D) Attempts to gain access to a protected system in violation of the act are punishable.

Oct/Nov 2014

**43.** Digital Rights Management (DRM) uses various methods to protect content. Which of the following is NOT an example of a DRM application?
(A) Blocking the forwarding of sensitive e-mails.
(B) Allowing peer-to-peer file software full access to all local storage drives.
(C) Restricting copying and printing of an e-book based on constraints.
(D) Including bits of information on a CD to confuse ripping software.

May/June 2010

**44.** A person commits computer crime if they perform certain actions without permission. Which of the following is an EXCEPTION to these specific acts?
(A) Securing access to a computer system.
(B) Introducing a computer contaminant.
(C) Denying access to an authorized person.
(D) Upgrading anti-virus software of a computer resource out of goodwill.

Oct/Nov 2022

**45.** What was the most appropriate rationale provided by the Supreme Court of India for striking down Section 66A of the IT Act?
(A) It failed to impose high enough fines for cyber terrorism.
(B) It disproportionately invaded the right of free speech under Article 19(1).
(C) It contradicted the provisions of the Bankers' Books Evidence Act.
(D) It was incompatible with the new DRM tracking technologies.

May/June 2013

**46.** Which of the following statements about the confiscation provisions under the Information Technology (IT) Act is incorrect?
(A) Any computer or floppy in respect of which a provision of the IT Act is contravened is liable to confiscation.
(B) Confiscation of a computer system completely immunizes the offender from any further penal imprisonment.
(C) Banks must take protective steps to prevent their systems from being misused to avoid confiscation.
(D) Section 76 deals specifically with the rules of confiscation.

Oct/Nov 2018

**47.** What is the most appropriate primary benefit of the amendment to the Indian Evidence Act, 1872 for Banks?
(A) It validates electronic records as evidence, allowing banks to remove bulky physical files.
(B) It allows banks to impose harsher penalties for loan defaults.
(C) It provides banks with the authority to issue arrest warrants for cyber criminals.
(D) It exempts banks from complying with the IT Rules, 2021.

May/June 2007

**48.** Which statement is incorrect regarding India's stance on Digital Rights Management (DRM) and International Treaties?
(A) The copyright law of India incorporates DRM provisions through the 2012 amendment.
(B) India is a primary signatory to the WIPO Copyright Treaty.

Downloaded from www.pdf.tube

(C) India incorporates provisions of international documents to be in line with international copyright standards.
(D) The 2012 amendment addresses the legal regime of copyright protection for digital media.

**Oct/Nov 2025**

**49.** Under the IT Rules, 2021, large digital platforms are required to produce monthly compliance reports. Which platform is NOT explicitly identified in the IT Rules, 2021 as a large platform (Significant Social Media Intermediary)?
(A) Signal
(B) WhatsApp
(C) Twitter
(D) Instagram

**May/June 2012**

**50.** Section 43 of the IT Act provides for compensation up to Rs. 1 crore for all of the following offences EXCEPT:
(A) Unauthorized Access.
(B) Introduction of a computer virus.
(C) Sending defamatory emails.
(D) Denial of Service (DoS).

**Oct/Nov 2023**

**51.** As per the salient features of the Information Technology (IT) Act, what is the most appropriate definition of a cyber cafe?
(A) An exclusive government agency that investigates cybercrimes.
(B) A residential hub for private network administration and data hosting.
(C) A facility provided to the public in the course of business for accessing the internet.
(D) A protected system maintained under the direct supervision of Section 70.

**May/June 2018**

**52.** Which statement regarding Section 74 of the IT Act is incorrect?
(A) It deals with publication for a fraudulent purpose.
(B) It carries a penalty of up to 2 years in prison or a fine.
(C) It is part of the offenses outlined under the IT Act 2000.
(D) It explicitly covers the creation of physical counterfeit currency.

**Oct/Nov 2016**

**53.** Which of the following is NOT an alternative name for Cyber law used internationally?
(A) Computer Misuse Act
(B) Computer Crime and Abuse
(C) Analog Transaction Act
(D) Electronic Transaction Act

**May/June 2014**

**54.** Why is the disclosure of an electronic record by a person in lawful possession considered a computer crime, particularly for bankers?
(A) Because electronic records use up vital server storage.
(B) Because customer account information and particulars must remain confidential.
(C) Because it avoids the application of Section 43 penalty clauses.
(D) Because the Indian Evidence Act prohibits banks from presenting electronic data in court.

**Oct/Nov 2007**

**55.** Confiscation under Section 76 applies to computers and accessories. Which condition is an EXCEPTION where confiscation does not apply?
(A) When a system is used exclusively for lawful banking business in compliance with regulations.
(B) When an accessory is used in direct contravention of the Information Technology Act.
(C) When a floppy disk contains a computer virus that was introduced intentionally.
(D) When a tape drive is utilized for the purpose of unauthorized data alteration.

**May/June 2025**

**56.** Which of the following statements comparing Section 65 and Section 66 of the IT Act is incorrect?
(A) Section 66 specifically mandates a mandatory 10-year prison sentence for a first-time hacking offence.
(B) Section 65 deals with tampering with computer source documents.
(C) Section 66 covers unauthorized alteration of data and hacking.
(D) An offence under Section 65 is punishable with up to 3 years in prison or a fine of up to Rs. 2 lakh.

NODIA

(D) All (I), (II), (III), and (IV)

**May/June 2022**

**82.** Consider the following statements regarding the retention of electronic records:

I The information must remain accessible for subsequent reference.

II The record must be retained in the format in which it was generated or received.

III The record must be printed and physically filed within 30 days.

Which combination of the above conditions must be met for the retention of electronic records to be valid?

(A) Only (II) and (III)
(B) Only (I) and (II)
(C) Only (I) and (III)
(D) All (I), (II), and (III)

**May/June 2016**

**83.** Consider the following statements regarding the acknowledgement of receipt of an electronic record:

I If the originator requests it, receipt must be acknowledged.

II If no method is agreed upon, acknowledgement may be given by any communication.

III Any conduct of the addressee indicating receipt is sufficient.

IV Acknowledgement is legally void if not digitally signed by a Certifying Authority.

Which of the above statement(s) correctly describes the rules for acknowledgement?

(A) Only (I), (II), and (IV)
(B) Only (I), (II), and (III)
(C) Only (II), (III), and (IV)
(D) All (I), (II), (III), and (IV)

**Oct/Nov 2009**

**84.** Consider the following statements regarding cyber offences under the Information Technology (IT) Act:

I Hacking with a computer system falls under Section 66.

II Introduction of malicious code causing data loss falls under Section 66.

III Denial of Service (DoS) is exclusively penalized under the IPC.

Which of the above statement(s) identifies the correct sections for the specified offences?

(A) Only (II) and (III)
(B) Only (I) and (III)
(C) Only (I) and (II)
(D) All (I), (II), and (III)

**Oct/Nov 2014**

**85.** Consider the following statements about court directions for digital signature verification:

I The court may direct the Controller or the Certifying Authority to produce the Digital Signature Certificate.

II The court cannot direct any other person to apply the public key listed in the certificate to verify the signature.

Which of the above statement(s) is/are correct?

(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**May/June 2010**

**86.** Match the amended Act in List I with its resultant benefit in List II due to the Information Technology Act 2000.

List I: (Amended Act)

P. Indian Penal Code
Q. Indian Evidence Act
R. Banker's Book of Evidence Act
S. Negotiable Instruments Act

List II: (Resultant Benefit)

1. Not applicable under the IT Act exemptions
2. Covers defamatory emails under Section 500
3. Allows printouts of electromagnetically stored data as ordinary business books
4. Treats electronic records as documents for court inspection

(A) P-4, Q-2, R-1, S-3
(B) P-2, Q-4, R-3, S-1
(C) P-3, Q-1, R-4, S-2
(D) P-1, Q-3, R-2, S-4

**Oct/Nov 2022**

**87.** Match the Section in List I with its prescribed penalty in List II.

List I: (Section)

P. Section 70 (Protected system access)
Q. Section 71 (Misrepresentation)
R. Section 74 (Publication for fraudulent purpose)
S. Section 43 (Unauthorized access)

List II: (Penalty)

1. Penalty of up to 2 years in prison or a fine

Click Here to Buy book on Amazon

compensation up to Rs. 1 crore
4. Involves executing instructions that spoil performance or attach to another computer

(A) P-4, Q-3, R-2, S-1
(B) P-2, Q-4, R-1, S-3
(C) P-3, Q-1, R-4, S-2
(D) P-1, Q-2, R-3, S-4

**May/June 2005**

**64.** Consider the following statements regarding the Information Technology (IT) Rules, 2021:
I They replaced the earlier IT (Intermediary Guidelines) Rules, 2011.
II They require digital portals to have a grievance redressal procedure.
III Platforms with more than 5 million users are exempt from monthly compliance reports.
Which of the above statement(s) is/are correct?
(A) Only (I) and (III)
(B) Only (II) and (III)
(C) Only (I) and (II)
(D) All (I), (II), and (III)

**Oct/Nov 2024**

**65.** Identify the correctly matched pair regarding the Information Technology (IT) Act amendments and their focal introduction.
(A) 2008 Amendment - Penalties for child porn, cyber terrorism, and voyeurism
(B) 2000 Amendment - Grievance redressal for OTT platforms
(C) 2012 Amendment - Recognition of the Indian Trust Act
(D) 2021 Amendment - Striking down of Section 66A

**May/June 2017**

**66.** Consider the following statements as listed in the Information Technology (IT) Act:
I Section 65 deals with tampering with computer source documents.
II Section 66 deals with hacking punishable by up to 3 years in prison.
III Section 67 deals with publishing obscene information in electronic form.
IV Section 68 deals with the controller's authority to issue orders.
Which of the above correctly matches the gist provided in the IT Act?
(A) All (I), (II), (III), and (IV)
(B) Only (I), (II), and (III)
(C) Only (I), (III), and (IV)
(D) Only (II), (III), and (IV)

**Oct/Nov 2005**

**67.** Consider the following legal milestones regarding Information Technology in India. Which of the following is the correct chronological sequence?
I Amendment enabling DRM through Copyright provisions
II Framing of new IT Rules requiring grievance redressal for OTT platforms
III Enactment of the original IT Act
IV Amendment introducing Section 66A and Section 69
(A) (III), (IV), (I), (II)
(B) (III), (I), (IV), (II)
(C) (IV), (III), (II), (I)
(D) (I), (III), (IV), (II)

**May/June 2020**

**68.** Consider the following statements regarding the issuance of a Digital Signature Certificate:
I The applicant must hold the private key corresponding to the public key to be listed in the certificate.
II The Certifying Authority is not required to record reasons in writing if an application is rejected.
Which of the above statement(s) is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**Oct/Nov 2015**

**69.** Consider the following statements regarding a Computer Contaminant:
I It is a set of computer instructions designed to modify or destroy data.
II It must be introduced physically via a USB floppy drive.
III It can usurp the normal operation of a computer system or network.
Which of the above statement(s) accurately reflects the definition of a Computer Contaminant?
(A) Only (I) and (III)
(B) Only (I) and (II)
(C) Only (II) and (III)
(D) All (I), (II), and (III)

NODIA

III Second conviction for publishing obscene info: up to 10 years.
IV Misrepresentation penalty: up to 2 years.
V Failure to comply with controller's orders: up to 5 years.

Which of the above statement(s) correctly identifies the specific imprisonment terms under the IT Act?
(A) Only (I), (II), (IV), and (V)
(B) Only (II), (III), (IV), and (V)
(C) Only (I), (II), (III), and (IV)
(D) All (I), (II), (III), (IV), and (V)

**May/June 2019**

**94.** An accountant hacks the bank's system and alters transaction data to cover embezzlement. What is the maximum recommended prison term?
(A) 1 year
(B) 5 years
(C) 3 years
(D) 10 years

**Oct/Nov 2006**

**95.** Select the correct option for the following Assertion (A) and Reason (R):
Assertion (A): The Information Technology (IT) Act 2000 has extraterritorial jurisdiction.
Reason (R): If an offence involves a computer system located in India, the offender is subject to prosecution under the Act, regardless of their nationality.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2021**

**96.** A student bypasses the firewall of a government server declared as a "protected system". Under which section will the student be penalized?
(A) Section 65
(B) Section 70
(C) Section 67
(D) Section 72

**Oct/Nov 2010**

**97.** Select the correct option for the following Assertion (A) and Reason (R):
Assertion (A): Banks are encouraged to dispense with the old system of maintaining bulky physical records.
Reason (R): The Indian Evidence Act, 1872 was amended to treat electronic records and printouts of electromagnetically stored data as legal documents for court inspection.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2005**

**98.** A bank implements an internal portal for branch managers to authenticate notes. Based on the IT Act, how is this authentication legally satisfied?
(A) By using a Digital Signature, governed by the Central Government's rules.
(B) By requiring a physical seal on a printout of the note before internal filing.
(C) By bypassing authentication since internal bank notes are not legally binding.
(D) By submitting the notes directly to the Cyber Regulations Advisory Committee.

**Oct/Nov 2023**

**99.** During a court case, a bank submits a printout of a ledger stored on an electromagnetic tape drive. Does the court recognize this?
(A) No, only handwritten ledgers are recognized by the court in loan default cases.
(B) Yes, due to amendments allowing electromagnetically stored data as evidence.
(C) No, because tape drives are excluded from the IT Act evidence amendments.
(D) Yes, but only if verified personally by the Deputy Superintendent of Police.

**May/June 2018**

**100.** Select the correct option for the following Assertion (A) and Reason (R):
Assertion (A): Section 66A of the IT Act continues to actively penalize offensive messages today.
Reason (R): The Supreme Court of India ruled that Section 66A arbitrarily and

Downloaded from www.pdf.tube

May/June 2008

**76.** Match the legal concept in List I with its implication in List II.

List I: (Legal Concept)

P. Legal Recognition of Electronic Records
Q. Acknowledgement of Receipt
R. Legal Recognition of Digital Signature
S. Submission of Forms in Electronic means

List II: (Implication)

1. Validates authentication by affixing a digital signature
2. Enables electronic maintenance of bank records
3. Facilitates e-banking through online account opening
4. Can be confirmed by any conduct indicating the record was received

(A) P-1, Q-3, R-2, S-4
(B) P-3, Q-1, R-4, S-2
(C) P-4, Q-2, R-3, S-1
(D) P-2, Q-4, R-1, S-3

Oct/Nov 2013

**77.** Consider the following statements regarding investigation and confiscation under the IT Act:

I Any computer system contravening IT Act rules is liable to confiscation.
II The Act gives the power to the Government to investigate offences.
III Only a Sub-Inspector can investigate cybercrimes under the Act.

Which of the above statement(s) is/are true?

(A) Only (I) and (III)
(B) Only (II) and (III)
(C) All (I), (II), and (III)
(D) Only (I) and (II)

May/June 2015

**78.** Match the Act in List I with its specific subject matter excluded from the IT Act in List II.

List I: (Act)

P. Indian Succession Act, 1925
Q. Negotiable Instruments Act, 1881
R. India Trust Act
S. Transfer of Property laws

List II: (Subject Matter)

1. Executing a Will
2. Document executing a negotiable instrument
3. Creating a trust
4. Contract for the sale of immovable property or interest in it

(A) P-2, Q-1, R-4, S-3
(B) P-3, Q-4, R-1, S-2
(C) P-4, Q-3, R-2, S-1
(D) P-1, Q-2, R-3, S-4

Oct/Nov 2012

**79.** Consider the following statements regarding penalties under the Information Technology (IT) Act:

I Penalties or confiscation imposed under the IT Act shall prevent the imposition of any other punishment to which the person is liable under any other law.
II A police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act.

Which of the above statement(s) is/are correct?

(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

May/June 2011

**80.** Identify the INCORRECTLY matched pair of Act and its subject matter impacted by the IT Act 2000.

(A) Indian Evidence Act, 1872 - Treats electronic records as documents
(B) Banker's Book of Evidence Act, 1891 - Includes printouts of electromagnetically stored data
(C) Indian Penal Code, 1860 - Governs penalties for defamatory emails
(D) Reserve Bank of India Act, 1934 - Regulates the physical confiscation of computer floppy disks

Oct/Nov 2020

**81.** Consider the following statements regarding Digital Rights Management (DRM) concepts:

I It uses encryption and digital watermarks as secure distribution mechanisms.
II It controls content exploitation by meta tagging.
III It relies on license rights established prior to encryption.
IV It functions by arresting offenders under Section 66A.

Which of the above statement(s) is/are correct?

(A) Only (II), (III), and (IV)
(B) Only (I), (III), and (IV)
(C) Only (I), (II), and (III)

NODIA

Oct/Nov 2019

**57.** What is the most appropriate condition under which the government may instruct subscribers to help intercept or decrypt information?
(A) During routine tax audits of private companies.
(B) If it is essential in the national interest to intercept computer resource information.
(C) When evaluating consumer credit loan proposals.
(D) To enforce compliance with WIPO DRM treaties.

May/June 2009

**58.** Which statement incorrectly describes the applicability of the Information Technology (IT) Act 2000?
(A) It applies to the execution of a Will under the Indian Succession Act, 1925.
(B) It covers the entire country of India.
(C) It has extraterritorial jurisdiction regardless of the offender's nationality.
(D) It provides legal recognition to electronic records.

Oct/Nov 2011

**59.** What is the most appropriate objective of the rules prescribed by the Central Government regarding the format of Digital Signatures?
(A) To generate revenue through the mandatory sale of digital keys.
(B) To ensure adequate integrity, security, and confidentiality of electronic records or payments.
(C) To bypass the judicial system when dealing with cybercrime.
(D) To eliminate the use of physical branches in the banking sector.

May/June 2019

**60.** Under the scope of Data Theft, which of the following is NOT covered?
(A) Diminishing the value of electronic data through theft.
(B) Physical theft of a banker's physical cash book.
(C) Theft of source or object code under Section 65.
(D) Punishments under Section 66 for hacking.

Oct/Nov 2006

**61.** Match the Digital Rights Management (DRM) application in List I with its practical example in List II.
List I: (DRM Application)
P. E-book server
Q. Movie studio DVD software
R. Company servers
S. Music label CD
List II: (Practical Example)
1. Blocks the forwarding of sensitive e-mail
2. Restricts access to, copying, and printing based on constraints
3. Limits the number of copies a user can make to two
4. Includes bits of information intended to confuse ripping software
(A) P-3, Q-2, R-4, S-1
(B) P-1, Q-4, R-2, S-3
(C) P-2, Q-3, R-1, S-4
(D) P-4, Q-1, R-3, S-2

May/June 2021

**62.** Consider the following statements regarding the 2008 amendment to the Information Technology (IT) Act:
I Section 66A was introduced to penalize offensive messages, but was later struck down by the Supreme Court.
II Section 69 was introduced giving authorities the power of interception, monitoring, or decryption.
Which of the above statement(s) is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

Oct/Nov 2010

**63.** Match the specific computer crime action in List I with its defining characteristic in List II.
List I: (Computer Crime Action)
P. Introducing a virus
Q. Unauthorized access
R. Data Alteration
S. Publishing obscene information
List II: (Defining Characteristic)
1. Penalized under Section 67 with up to 5 years prison for first conviction
2. Dealt with under Section 66 regarding hacking
3. Addressed under Section 43 with

Click Here to Buy book on Amazon

2. Compensation of up to Rs. 1 crore
3. Punishable by 2 years in prison and a fine of Rs. 1 lakh
4. Subject to imprisonment and a fine for violating system access

(A) P-4, Q-3, R-1, S-2
(B) P-3, Q-4, R-2, S-1
(C) P-1, Q-2, R-3, S-4
(D) P-2, Q-1, R-4, S-3

**May/June 2013**

**88.** Match the legal issue in List I with its corresponding section/provision in List II.

List I: (Legal Issue)
P. Data Theft
Q. Defamatory Emails
R. Breach of confidentiality
S. Intercepting in national interest

List II: (Section/Provision)
1. Section 66 of IT Act
2. Section 500 of IPC
3. Section 72 of IT Act
4. Implied under instructions to decrypt (Section 69)

(A) P-2, Q-1, R-4, S-3
(B) P-1, Q-2, R-3, S-4
(C) P-3, Q-4, R-1, S-2
(D) P-4, Q-3, R-2, S-1

**Oct/Nov 2018**

**89.** Match the Digital Rights Management (DRM) mechanism component in List I with its function in List II.

List I: (DRM Component)
P. Encryption
Q. Digital Watermarks
R. Secure Distribution
S. License rights

List II: (Function)
1. General mechanism used to track and copy protect content
2. Locks the content requiring decryption technology to unlock
3. Embedded markers tracking copyright ownership
4. Usage rules defining permitted exploitation of content

(A) P-1, Q-4, R-2, S-3
(B) P-3, Q-1, R-4, S-2
(C) P-4, Q-2, R-3, S-1
(D) P-2, Q-3, R-1, S-4

**May/June 2007**

**90.** Identify the INCORRECTLY matched pair of Section and its corresponding offense under the IT Act.

(A) Section 72 - Controller's authority to issue orders
(B) Section 65 - Tampering with computer source documents
(C) Section 67 - Publishing obscene information in electronic form
(D) Section 74 - Publication for a fraudulent purpose

**Oct/Nov 2025**

**91.** Select the correct option for the following Assertion (A) and Reason (R):

Assertion (A): Banks should not allow their computer systems to be used for purposes other than their banking business.

Reason (R): Any computer system or accessories in respect of which any provision of the IT Act is contravened shall be liable to confiscation.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2012**

**92.** An employee downloads a customer database without permission using a USB drive. Under the IT Act, what has the employee committed?

(A) A lawful data backup procedure commonly practiced in the finance sector.
(B) Publication for a fraudulent purpose under Section 74 of the IT Act.
(C) Computer Crime by downloading data without authorization from the owner.
(D) A violation of the World Intellectual Property Organization (WIPO) Copyright Treaty.

**Oct/Nov 2014**

**93.** Consider the following offences and their imprisonment terms:

I Tampering with source documents: up to 3 years.
II First conviction for publishing obscene info: up to 5 years.

Downloaded from www.pdf.tube

May/June 2023

**70.** Match the term in List I with its corresponding description in List II.

List I: (Term)

P. Computer Contaminant
Q. Certifying Authority
R. Meta tagging
S. Cyber terrorism penalty

List II: (Description)

1. Issues Digital Signature Certificates
2. Code that modifies, destroys, or transmits data
3. Introduced by the Amendment to IT Act in 2008
4. Process used in DRM prior to content being encrypted

(A) P-1, Q-2, R-3, S-4
(B) P-4, Q-3, R-2, S-1
(C) P-2, Q-1, R-4, S-3
(D) P-3, Q-4, R-1, S-2

Oct/Nov 2021

**71.** Consider the following salient features of the Information Technology (IT) Act:

I It elaborates on offenses, penalties, and breaches.
II It states that cyber cafe means a facility provided to the public in the course of business.
III It establishes the Cyber Regulations Advisory Committee.
IV Provision to section 81 states that acts have an overriding effect.

Which of the above statement(s) represent(s) the salient features of the IT Act?

(A) All (I), (II), (III), and (IV)
(B) Only (I), (II), and (III)
(C) Only (I), (II), and (IV)
(D) Only (II), (III), and (IV)

May/June 2024

**72.** Match the Section of the Information Technology (IT) Act in List I with the corresponding offense in List II.

List I: (Section)

P. Section 65
Q. Section 66
R. Section 68
S. Section 71

List II: (Offense)

1. Controller's authority to issue orders
2. Misrepresentation penalty
3. Tampering with computer source documents
4. Hacking with a computer system

(A) P-4, Q-3, R-2, S-1
(B) P-3, Q-4, R-1, S-2
(C) P-1, Q-2, R-3, S-4
(D) P-2, Q-1, R-4, S-3

NODIA

Oct/Nov 2008

**73.** Consider the following statements regarding email abuse under the IT Act:

I Sending pornographic emails is punishable with up to 5 years imprisonment and Rs. 1 lakh fine on first conviction.
II Threatening emails are punishable under Section 43 of the IT Act with a compensation of Rs. 1 crore.

Which of the above statement(s) is/are correct?

(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

May/June 2006

**74.** Identify the correctly matched pair between the Digital Rights Management (DRM) concept and its definition.

(A) Digital Watermark - A physical stamp required on electronic forms
(B) Meta tagging - Removing the copyright metadata from a file
(C) Decryption technology - Used to unlock content encrypted under DRM
(D) Peer-to-peer exchange - A secure distribution mechanism endorsed by DRM

Oct/Nov 2017

**75.** Consider the following actions related to computer systems:

I Secures access to a computer network.
II Downloads data from a removable storage medium.
III Denies access to an authorized person.
IV Charges services to another person's account by manipulating the system.

Which combination of actions constitutes a computer crime if performed without permission?

(A) Only (I), (II), and (III)
(B) Only (I), (III), and (IV)
(C) Only (II), (III), and (IV)
(D) All (I), (II), (III), and (IV)

disproportionately invades the right of free speech under Article 19(1).
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2016**

**101.** A corporation configures servers to block employees from forwarding "sensitive" emails externally. This is an application of which technology?
(A) Digital Rights Management (DRM)
(B) Denial of Service (DoS)
(C) Cryptographic key pair generation
(D) Cyber Regulations Advisory protocols

**May/June 2014**

**102.** Consider the following documents:
I A document executing a negotiable instrument.
II A power of execution of an attorney.
III The creation of a trust under the India Trust Act.
IV Executing a Will under the Indian Succession Act, 1925.
V A contract for the sale of immovable property.
Which combination of the above documents is explicitly excluded from the applicability of the Information Technology (IT) Act?
(A) All (I), (II), (III), (IV), and (V)
(B) Only (I), (II), (III), and (IV)
(C) Only (I), (III), (IV), and (V)
(D) Only (II), (III), (IV), and (V)

**Oct/Nov 2007**

**103.** As a System Auditor auditing a bank acting as a Certifying Authority, what technical assurance regarding keys must you verify?
(A) That the public and private keys are identical in their encrypted string format.
(B) That the subscriber holds the private key matching the public key in the pair.
(C) That the private key is held exclusively by the Certifying Authority at all times.
(D) That the keys can bypass Digital Rights Management (DRM) encryption protocols.

**May/June 2025**

**104.** Select the correct option for the following Assertion (A) and Reason (R):
Assertion (A): The System Auditor plays a role in verifying the Digital Signature Certificate issuance when banks act as Certifying Authorities.
Reason (R): The System Auditor ensures that the Certifying Authority has complied with the provisions of the IT Act, rules, and regulations.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2019**

**105.** An ISP refuses to comply with an order issued by the Controller. According to Section 68, what is the penalty?
(A) Five years in jail and confiscation of all assets.
(B) A fine of Rs. 1 crore only.
(C) Three years in jail and a fine.
(D) Ten years in prison.

**May/June 2009**

**106.** Consider the following acts as defined under the Information Technology (IT) Act:
I Hacking with a computer system.
II Misrepresentation to the Certifying Authority.
III Breach of confidentiality and privacy.
IV Publication for a fraudulent purpose.
V Legally retaining an electronic record for subsequent reference.
Which combination of acts is explicitly defined as an offence resulting in a penalty or confiscation?
(A) Only (I), (II), (III), and (V)
(B) Only (I), (II), (III), and (IV)
(C) Only (I), (III), (IV), and (V)
(D) All (I), (II), (III), (IV), and (V)

**Oct/Nov 2011**

**107.** A customer sends emails threatening a bank manager with physical harm. Which legal provision addresses this email abuse?
(A) IPC provisions pertaining to criminal

Click Here to Buy book on Amazon

intimidation and physical threats.
(B) Section 66A of the Information Technology (IT) Act 2000.
(C) Section 67 of the Information Technology (IT) Act 2000.
(D) Section 500 of the Indian Penal Code (IPC) regarding defamation.

**May/June 2010**

**108.** Select the correct option for the following Assertion (A) and Reason (R):
Assertion (A): If the introduction of a malicious code results in the loss of data, Section 66 of the IT Act will be applicable along with Section 43.
Reason (R): Section 43 covers compensation for malicious code introduction, and Section 66 covers unauthorized alteration and hacking of data.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2024**

**109.** Mr. B suppresses the fact that he has a prior cybercrime conviction while applying for a license. How is this action classified?
(A) An oversight not punishable under the IT Act.
(B) Data Theft under Section 66.
(C) A legitimate business tactic not covered by law.
(D) Misrepresentation, which is considered a committed computer crime.

**May/June 2017**

**110.** Select the correct option for the following Assertion (A) and Reason (R):
Assertion (A): Acts specified under the Information Technology (IT) Act 2000 have an overriding effect over other conflicting laws.
Reason (R): The provision under Section 81 of the IT Act explicitly states that the Act has an overriding effect.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2005**

**111.** A police station receives a complaint about sophisticated cyber fraud. Who is the minimum-ranked officer authorized to investigate this?
(A) Head Constable
(B) Sub-Inspector
(C) Inspector
(D) Deputy Superintendent of Police

**May/June 2020**

**112.** Select the correct option for the following Assertion (A) and Reason (R):
Assertion (A): DRM products were developed in response to the rapid increase in online piracy and peer-to-peer file exchange programs.
Reason (R): Digital Rights Management (DRM) aims to restrict the ways consumers can copy content they have purchased and prevent unauthorized redistribution.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2015**

**113.** Select the correct option for the following Assertion (A) and Reason (R):
Assertion (A): The copyright law of India incorporates the provisions of Digital Rights Management (DRM) to be in line with international standards.
Reason (R): India is a signatory to the World Intellectual Property Organization Copyright Treaty.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

NODIA

May/June 2023

**114.** A software developer's source code is stolen. Which section of the IT Act specifically deals with the theft of source or object code?
(A) Section 43
(B) Section 65
(C) Section 67
(D) Section 72

Oct/Nov 2021

**115.** Mr. A insists a bank must accept his loan processing fee electronically under the IT Act. What does the Act stipulate regarding this insistence?
(A) The Act mandates that all organizations must accept monetary transactions in electronic form upon customer insistence.
(B) The bank must accept it only if Mr. A provides a physical cheque alongside the digital transaction for record-keeping.
(C) The bank is required to confiscate Mr. A's computer if he insists on electronic payment without prior bank authorization.
(D) The Act does not grant the right to insist on electronic monetary transactions.

May/June 2024

**116.** Consider the following practical examples of content protection:
I Blocking the forwarding of sensitive e-mail.
II Restricting printing of an e-book.
III Limiting DVD software copies to two.
IV Including bits of information on a CD to confuse ripping software.
V Publishing a daily list of cybercriminals in the newspaper.
Which combination of examples demonstrates the practical application of Digital Rights Management (DRM)?
(A) Only (I), (II), (III), and (V)
(B) Only (II), (III), (IV), and (V)
(C) All (I), (II), (III), and (IV)
(D) Only (I), (II), (III), and (IV)

Oct/Nov 2008

**117.** A cybercriminal introduces a Trojan that deletes terabytes of financial data. Which sections of the IT Act are applicable?
(A) Only Section 43.
(B) Only Section 67.
(C) Section 70 and Section 74.
(D) Section 43 and Section 66.

May/June 2006

**118.** Select the correct option for the following Assertion (A) and Reason (R):
Assertion (A): Disclosure of electronic records by a person in lawful possession to an unauthorized person constitutes a computer crime.
Reason (R): Bankers maintain sensitive information regarding accounts, and customer secrecy is a paramount obligation protected under these provisions.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Oct/Nov 2017

**119.** A hacker creates and publishes a forged Digital Signature Certificate to secure a massive corporate loan. What is the classification of this act?
(A) A Computer Crime, as creating or publishing a DSC for fraudulent purpose.
(B) A breach of the Indian Trust Act regarding the creation of unauthorized records.
(C) Misrepresentation to the Controller as specifically defined under Section 71.
(D) A civil dispute falling outside the scope of the Information Technology Act.

May/June 2008

**120.** Select the correct option for the following Assertion (A) and Reason (R):
Assertion (A): The Information Technology (IT) Act 2000 has extraterritorial jurisdiction.
Reason (R): If an offence involves a computer system located in India, the offender is subject to prosecution under the Act, regardless of their nationality.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Downloaded from www.pdf.tube

privacy. It specifically penalizes any person who, having secured access to any electronic record, book, register, or document without the consent of the person concerned, discloses such information. Violations of this section are punishable with imprisonment, a fine, or both.

**26.** (D) Source or object code.
In the context of computer-related offences, data theft extends beyond simple information to include technical assets. The Information Technology Act explicitly includes computer source code or object code as objects of theft. Section 65 specifically deals with the tampering of these documents, recognizing them as valuable intellectual property that is essential for the functioning of computer systems and software programmes.

**27.** (A) Anyone who fails to comply will be sentenced to three years in jail and a fine.
Section 68 of the Information Technology Act empowers the Controller to issue specific orders to Certifying Authorities or their employees to ensure compliance with the Act. To ensure these orders are taken seriously, the law prescribes a penal consequence for non-compliance. Any person who fails to comply with such an order is liable to imprisonment for up to three years.

**28.** (A) February 25
The Union Government of India framed and notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, on February 25. These rules were introduced to regulate social media intermediaries, over-the-top platforms, and digital news publishers, establishing a comprehensive framework for grievance redressal and due diligence requirements for digital entities operating within the country.

**29.** (C) Information must remain accessible so as to be usable for subsequent reference.
For the retention of electronic records to be legally valid under the Information Technology Act, certain conditions must be satisfied. A primary requirement is that the information contained in the record must remain accessible. This accessibility ensures that the data can be retrieved and used for subsequent reference by authorized persons, maintaining the record's legal utility over time.

**30.** (D) Suppressing material facts or making misrepresentations to obtain a certificate.
A computer crime regarding misrepresentation occurs when a person provides false information to the Controller or a Certifying Authority. This includes the intentional suppression of material facts or making false statements with the intent to obtain a license or a Digital Signature Certificate. Such acts are penalized under Section 71 of the Information Technology Act to maintain system integrity.

**31.** (C) The foundational legal recognition of Digital Signatures.
The foundational legal recognition of Digital Signatures was established by the original Information Technology Act in 2000, not by the 2008 amendment. The 2008 amendment focused on expanding the Act's scope by introducing Section 66A for offensive messages, Section 69 for interception powers, and various penalties for modern cybercrimes such as cyber terrorism, voyeurism, and child pornography.

NODIA

**32.** (C) Application form for opening a bank account electronically.
While the Information Technology Act provides legal recognition to many electronic documents, certain categories are explicitly excluded from its scope. These exclusions include negotiable instruments, powers of attorney, trusts, wills, and contracts for the sale of immovable property. However, application forms for opening bank accounts electronically are not excluded and are widely used within the e-banking framework today.

**33.** (B) Banks are strictly required to maintain physical forms of all data alongside electronic forms.
The amendment to the Banker's Book of Evidence Act, 1891, was designed to modernize the legal standing of bank records. It recognizes ledgers and cash books maintained in electronic forms, such as on floppy disks or magnetic tapes. Contrary to maintaining physical backups, the amendment allows banks to use certified printouts of these electronic records as primary evidence in court.

# ANSWERS

1. (D) Up to 3 years in prison, a fine of up to Rs. 2 lakh, or both.
   Section 65 of the Information Technology Act specifically addresses the offence of tampering with computer source documents. This section mandates that any individual who intentionally conceals, destroys, or alters source code used for a computer, computer programme, computer system, or computer network shall be punishable with imprisonment up to three years, a fine, or both.

2. (C) The requirement for digital platforms to have grievance procedures.
   The Information Technology Rules of 2021 introduced a significant regulatory framework for digital platforms and intermediaries operating within India. A central conceptual mandate of these rules requires platforms to establish robust grievance redressal mechanisms. This includes appointing a grievance officer to acknowledge and resolve user complaints within a specified timeframe to ensure accountability and user protection.

3. (C) Instructions or programs that degrade computer performance or attach to other resources.
   In the domain of computer crimes, a computer virus is technically defined as a set of instructions or programs. These malicious codes are specifically designed to attach themselves to other computer resources or programs. Their primary function is to degrade the performance of the system, destroy data, or modify existing instructions without the authorization of the user.

4. (C) Compensation is provided under Section 43, and Section 66 applies if data loss occurs.
   The introduction of a computer virus or contaminant is addressed through multiple sections of the Information Technology Act. Section 43 focuses on civil liability, allowing for compensation to be paid to the affected party. Furthermore, Section 66 is invoked for criminal prosecution if the introduction of such malicious code results in unauthorized data alteration or loss.

5. (B) It can be given by any conduct sufficient to indicate the record was received.
   When an originator and an addressee have not formally agreed upon a specific method for acknowledging the receipt of an electronic record, the law provides flexible alternatives. In such instances, the acknowledgement may be effectively given by any communication from the addressee or by any conduct that is sufficient to indicate to the originator that the record was received.

6. (B) They generally use Encryption and Digital Watermarks.
   Digital Rights Management employs secure distribution mechanisms to protect digital content from unauthorized access or redistribution. These mechanisms typically rely on sophisticated technical tools such as encryption, which locks the content for unauthorized users, and digital watermarks, which are embedded markers used to track ownership and identify the origin of the content across various digital platforms and networks.

7. (B) Accessible electronic records usable for subsequent reference.
   Legal recognition under the Information Technology Act is granted to electronic records based on their accessibility and utility. To be treated as valid, an electronic record must be stored or transmitted in a manner where the information contained therein remains accessible. This ensures that the data can be retrieved and used for subsequent reference by any person or authority.

8. (B) Unauthorized alteration of data punishable by imprisonment, fine, or both.
   Conceptually, the offence of hacking under Section 66 of the Information Technology Act involves the unauthorized alteration, destruction, or deletion of data within a computer resource. Such actions are regarded as

Click Here to Buy book on Amazon

criminal offences. The prescribed punishment for individuals found guilty of hacking includes a term of imprisonment, a financial fine, or both, depending on the severity of the act.

**9.** (B) Reasons for rejecting an application for a Digital Signature Certificate must be recorded in writing.
The Certifying Authority is empowered to issue Digital Signature Certificates upon verifying the applicant's credentials. However, this authority is balanced by procedural requirements to ensure transparency. If the Certifying Authority decides to reject an application for a certificate, it is legally mandated to record the specific reasons for such a rejection in writing and communicate them to the applicant.

**10.** (C) 24 March 2015
In a landmark judicial decision regarding digital freedom of speech, the Supreme Court of India delivered a significant verdict on 24 March 2015. In the case of Shreya Singhal vs. Union of India, the court struck down Section 66A of the Information Technology Act in its entirety, ruling that the provision was unconstitutional due to its vague and overbroad nature.

**11.** (D) It recognizes electronic data interchange and filing as legally valid means.
The Information Technology Act was enacted to provide a legal framework for electronic commerce and digital transactions. A primary objective achieved by this Act is the legal recognition of electronic data interchange and the electronic filing of documents with government agencies. This recognition allows digital records to hold the same legal standing as traditional paper-based documents in various commercial transactions.

**12.** (C) Systems protecting digital media from unauthorized redistribution.
Digital Rights Management refers to a set of technologies and systemic procedures designed to protect digital media and intellectual property. The fundamental definition of these systems centers on controlling how users access, use, and redistribute digital content. By implementing these controls, content creators and distributors can prevent unauthorized copying and ensure that digital assets are exploited only according to license.

**13.** (A) By meta tagging content with relevant usage rules prior to the content being encrypted.
Digital Rights Management systems control the exploitation of digital content through a structured technical process. Before the content is secured via encryption, it undergoes meta tagging. This involves embedding specific usage rules and license rights directly into the metadata of the file. These tags then dictate the permitted actions, such as viewing, printing, or copying, once the content is decrypted.

NODIA

**14.** (C) It allows electronic account opening, removing the need for physical submission.
The legal framework for submitting forms by electronic means significantly facilitates the expansion of e-banking services. This provision conceptually allows customers to perform various banking activities, such as opening new accounts, entirely through digital channels. By granting legal validity to electronic forms, the requirement for customers to physically visit a bank branch to submit paper-based documents is effectively removed.

**15.** (D) It introduced Section 66A which penalized "offensive messages".
The Information Technology (Amendment) Act of 2008 introduced several new provisions to address emerging cyber threats. One notable introduction was Section 66A, which was designed to penalize the sending of "offensive messages" through communication services. Although this specific section was later struck down by the Supreme Court, its introduction in 2008 represented a significant expansion of the original Act.

**16.** (A) Instructions designed to damage, destroy, or usurp computer operations.
According to the Information Technology Act, a computer contaminant is defined as a set of computer instructions. These instructions are specifically engineered to modify, damage, destroy, record, or transmit data without authorization. They are also designed to usurp the normal operation of a computer, computer system, or network, thereby compromising the

integrity and performance of the targeted digital resource.

17. (D) The court may direct any other person to apply the public key listed in the certificate and verify the digital signature.
In legal proceedings involving the verification of a digital signature, the court possesses specific powers under the Indian Evidence Act. The court may direct the person who affixed the signature, or the Controller/Certifying Authority, to produce the relevant certificate. Additionally, the court has the authority to direct any person to apply the public key to verify the digital signature.

18. (A) Imprisonment up to 10 years and fine up to Rs. 2 lakh.
Section 67 of the Information Technology Act deals with the publication or transmission of obscene material in electronic form. The law distinguishes between initial and subsequent offences to deter repeat violators. For a second or subsequent conviction involving the transmission of pornographic or obscene emails, the recommended punishment increases significantly to imprisonment for up to ten years and a heavy fine.

19. (D) The United Nations' model law.
The enactment of the Information Technology Act 2000 in India was based on an international legal foundation. It was developed to align with the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. This foundational model provided the conceptual framework for recognizing electronic records and signatures, ensuring consistency with global digital trade standards.

20. (A) Section 500 of the Indian Penal Code (IPC).
Although the Information Technology Act addresses various cybercrimes, certain offences involving digital communication are governed by the Indian Penal Code. Emails that are defamatory in nature, which involve making false statements to harm a person's reputation, are punishable under Section 500 of the Indian Penal Code. This ensures that traditional legal protections against defamation apply to the digital medium.

21. (C) Large platforms must produce monthly reports on complaints received and actions taken.
Under the Information Technology Rules of 2021, significant social media intermediaries with a large user base are subject to specific transparency requirements. These large digital platforms are mandated to publish monthly compliance reports. These reports must include details regarding the number of complaints received from users in India and the specific actions taken by the platform to address those grievances.

NODIA

22. (B) 94 sections, 13 chapters, and 4 schedules.
The original Information Technology Act, as enacted in 2000, was structured into a specific legislative format to cover a wide range of digital legalities. This structure consisted of 94 sections organized across 13 chapters. Additionally, the Act included 4 schedules that detailed various amendments to existing laws, such as the Indian Penal Code and the Indian Evidence Act.

23. (D) Signatures are recognized if authenticated by means prescribed by the government.
The legal recognition of a digital signature is conceptually rooted in the method of authentication used for electronic records. According to the Information Technology Act, a digital signature is considered legally valid if it is authenticated by the use of asymmetric crypto systems and hash functions, or any other authentication method as prescribed by the Central Government from time to time.

24. (A) Defamatory emails are under IPC 500, while threats fall under IPC intimidation.
Email abuse is categorized into different legal violations based on the nature of the content sent. Defamatory emails, which damage an individual's reputation, are prosecuted under Section 500 of the Indian Penal Code. Conversely, emails containing threats of physical harm are addressed under the provisions for criminal intimidation within the Indian Penal Code, rather than the Information Technology Act.

25. (B) By penalizing the breach of confidentiality and privacy with fines and imprisonment.
Section 72 of the Information Technology Act provides conceptual protection to users by upholding the principles of confidentiality and

resources designated as such by the government. The penalties for unauthorized access to these systems are severe and are not limited to financial compensation. Instead, individuals who secure or attempt to secure unauthorized access to a protected system are subject to criminal penalties, including significant imprisonment and fines.

**43.** (B) Allowing peer-to-peer file software full access to all local storage drives.
Digital Rights Management applications are designed to restrict and control the use of digital content. Examples include blocking email forwarding, restricting e-book printing, and adding data to CDs to confuse ripping software. Conversely, allowing peer-to-peer software full access to local drives facilitates unauthorized redistribution, which is the exact opposite of what Digital Rights Management systems are intended to achieve.

**44.** (D) Upgrading anti-virus software of a computer resource out of goodwill.
Under the Information Technology Act, a computer crime involves performing specific acts without the owner's permission, such as securing unauthorized access, introducing contaminants, or denying service to authorized users. Upgrading anti-virus software, even if done out of goodwill, is not typically categorized as one of these specific offences, provided it does not involve unauthorized access or alteration of the system's data.

**45.** (B) It disproportionately invaded the right of free speech under Article 19(1).
When the Supreme Court of India struck down Section 66A of the Information Technology Act, it provided a clear constitutional rationale. The court determined that the provision was vague and overbroad, leading to a "chilling effect" on communication. Ultimately, it was ruled that Section 66A disproportionately and arbitrarily invaded the fundamental right to freedom of speech guaranteed under Article 19(1) of the Constitution.

**46.** (B) Confiscation of a computer system completely immunizes the offender from any further penal imprisonment.
The confiscation provisions under Section 76 of the Information Technology Act allow for the seizure of computer systems involved in contraventions. However, such confiscation does not provide immunity from other legal consequences. An offender whose equipment is confiscated can still face separate penal sentences, such as imprisonment or fines, as prescribed by the relevant sections of the Act or other laws.

**47.** (A) It validates electronic records as evidence, allowing banks to remove bulky physical files.
The amendment to the Indian Evidence Act, 1872, provides a major benefit to the banking sector by validating electronic records as legal evidence. This legal shift allows banks to move away from maintaining massive, bulky physical ledgers and files. Instead, they can rely on digitally stored data and printouts, which are now recognized as admissible documents for inspection by the courts.

**48.** (B) India is a primary signatory to the WIPO Copyright Treaty.
India has updated its copyright laws, specifically through the 2012 amendment, to include Digital Rights Management provisions that align with international standards. While India incorporates elements from international documents like the WIPO Copyright Treaty to address the legal regime of digital media protection, it is important to note that India is a primary signatory to the WIPO Copyright Treaty.

**49.** (A) Signal
The Information Technology Rules of 2021 identify significant social media intermediaries based on their user base in India. Platforms like WhatsApp, Twitter, and Instagram, which have millions of users, are explicitly subject to the transparency and compliance reporting requirements of these rules. Signal, while a popular communication platform, is not explicitly highlighted as a significant social media intermediary within these specific rules.

**50.** (C) Sending defamatory emails.
Section 43 of the Information Technology Act provides for civil compensation up to one crore rupees for various computer-related offences, including unauthorized access, introduction of viruses, and denial of service. However, sending defamatory emails is handled differently. Defamation is primarily a criminal offence under

Downloaded from www.pdf.tube

**34.** (A) Actions that deny access to any person authorized to use a computer network.
Under the Information Technology Act, a Denial of Service attack refers to an intentional act performed without the permission of the owner or person in charge. This offence involves performing actions that result in the denial of access to any person who is otherwise authorized to use a computer resource, computer system, or a computer network, thereby disrupting normal operations.

**35.** (A) The disclaimer stating that IT Act provisions do not confer rights to insist on electronic monetary payments.
While the Information Technology Act grants legal recognition to electronic records and signatures, it contains a specific limitation regarding their mandatory acceptance. The Act includes a disclaimer clarifying that these provisions do not confer a legal right upon any person to insist that a government department or an organization must accept, issue, or process documents or monetary payments in electronic form.

**36.** (A) To make content theft technically impossible rather than relying on legal actions after the fact.
Digital Rights Management aims to shift the focus from reactive legal prosecution to proactive technical prevention. Unlike traditional copyright laws, which provide a legal basis for action after an infringement has occurred, the primary goal of Digital Rights Management is to implement technical barriers. These barriers are intended to make the unauthorized copying or redistribution of digital content technically impossible or extremely difficult.

**37.** (A) Without an agreed method, a record is deemed undelivered regardless of conduct.
The rules regarding the acknowledgement of receipt of electronic records allow for flexibility when no specific method has been agreed upon. In such cases, the record is not automatically deemed undelivered. Instead, the law recognizes that acknowledgement can be given through any communication or conduct by the addressee that is sufficient to indicate to the originator that the record was received.

**38.** (D) Breaching Indian Trust Act rules through electronic contract creation.
The Information Technology Act 2000 lists several salient offences, including tampering with source documents, misrepresentation to the Controller, and unauthorized access to protected systems. However, the creation of electronic contracts related to trusts is generally excluded from the Act's applicability. Therefore, breaching Indian Trust Act rules through electronic contract creation is not a listed offence under the Information Technology Act's framework.

**39.** (B) Acting as a Certifying Authority.
In the evolving environment of e-business, banks have the opportunity to take on new functional roles related to digital security. One of the most appropriate primary roles for banks is to act as a Certifying Authority. In this capacity, banks can issue Digital Signature Certificates to their customers, thereby facilitating secure electronic transactions and reinforcing trust in digital banking services.

NODIA

**40.** (D) Negotiable Instruments Act.
The Information Technology Act 2000 brought about significant changes to several existing statutes to accommodate the digital age. These amendments specifically impacted the Indian Penal Code, the Indian Evidence Act, and the Bankers' Books Evidence Act. However, the Negotiable Instruments Act was not among the primary acts fundamentally amended by the Information Technology Act for the purpose of digital recognition.

**41.** (B) (II), (IV), (III), (I)
To understand the legal landscape, it is helpful to arrange the relevant Acts chronologically by their original enactment dates. The Indian Penal Code was enacted first in 1860, followed by the Indian Evidence Act in 1872. The Bankers' Books Evidence Act was subsequently enacted in 1891. Finally, the Information Technology Act was enacted much later, at the turn of the millennium in 2000.

**42.** (C) The penalty under this section is strictly limited to financial compensation up to Rs. 1 crore.
Section 70 of the Information Technology Act addresses protected systems, which are computer

Oct/Nov 2013

**121.** An NRI wishes to execute a Power of Attorney electronically. Does the Information Technology (IT) Act 2000 legally validate this document?
(A) Yes, because it involves banking operations for international accounts.
(B) Yes, because digital signatures have universal legal recognition in India.
(C) No, the Information Technology (IT) Act applies only to resident citizens.
(D) No, the Act does not apply to a power of execution of an attorney.

May/June 2015

**122.** A consumer is unable to print a purchased e-book due to software restrictions. What aspect of DRM is functioning here?
(A) The introduction of a computer contaminant via a remote host.
(B) The execution of a Digital Signature for user verification.
(C) The enforcement of license rights and usage rules on the content.
(D) The interception of communications in the interest of national security.

Oct/Nov 2012

**123.** A foreign national residing in Europe hacks into a server located in Mumbai. Can they be prosecuted under the IT Act 2000?
(A) No, the Act strictly applies only to Indian citizens residing in the country.
(B) No, the jurisdiction is restricted to offences committed geographically on Indian soil.
(C) Yes, the Act has extraterritorial jurisdiction for systems located in India.
(D) Yes, but only under the WIPO treaties, not the Information Technology Act.

May/June 2011

**124.** A social media platform with 6 million users fails to produce a required monthly compliance report. Under which framework are they in violation?
(A) The Information Technology (IT) Rules, 2021.
(B) The IT (Intermediary Guidelines) Rules, 2011.
(C) Section 66A of the Information Technology (IT) Act.
(D) The World Intellectual Property Organization (WIPO) Copyright Treaty.

Oct/Nov 2020

**125.** Two parties attempt to enter a contract for the sale of immovable property electronically. Is this contract valid under the Act?
(A) Yes, because the Act recognizes all electronic data interchange methods.
(B) No, the Act is not applicable to contracts for the sale of immovable property.
(C) Yes, provided the platform uses certified Digital Rights Management (DRM).
(D) No, unless the Controller issues a specific order authorizing the sale.

www.nodia.in

Click Here to Buy book on Amazon

Section 500 of the Indian Penal Code and does not fall under the compensation framework of Section 43.

**51.** (C) A facility provided to the public in the course of business for accessing the internet.
Within the salient features of the Information Technology Act, a cyber cafe is clearly defined. It refers to any facility provided by a person to the public in the course of their business that allows users to access the internet. This definition ensures that such businesses are recognized as intermediaries and are subject to the relevant regulations and due diligence requirements.

**52.** (D) It explicitly covers the creation of physical counterfeit currency.
Section 74 of the Information Technology Act deals with the offence of publication for a fraudulent purpose. It specifically penalizes the creation, publication, or making available of a Digital Signature Certificate for any fraudulent or unlawful purpose. This section is strictly focused on digital records and electronic certificates; it does not cover the physical creation of counterfeit paper currency or similar physical crimes.

**53.** (C) Analog Transaction Act
Cyber law is known by several alternative names across different international jurisdictions. Common terms include the Computer Misuse Act, Electronic Transaction Act, and regulations concerning Computer Crime and Abuse. However, the term "Analog Transaction Act" is not used to describe cyber law, as these laws are specifically designed to address digital and electronic environments rather than traditional analog systems or transactions.

**54.** (B) Because customer account information and particulars must remain confidential.
The disclosure of electronic records by a person in lawful possession is considered a serious computer crime, especially for bankers. This is because banks are entrusted with sensitive customer account information and personal particulars. Maintaining customer secrecy is a paramount legal and ethical obligation. Unauthorized disclosure violates the privacy of the customer and undermines the trust essential to the banking system.

**55.** (A) When a system is used exclusively for lawful banking business in compliance with regulations.
Confiscation under Section 76 of the Information Technology Act applies to computer systems and accessories involved in a contravention. An exception exists when the system is used for lawful purposes. If a bank ensures its systems are used exclusively for legitimate banking business in compliance with all relevant regulations, those systems are generally protected from confiscation, provided they were not misused.

**56.** (A) Section 66 specifically mandates a mandatory 10-year prison sentence for a first-time hacking offence.
Comparing the two sections, Section 65 deals with tampering with computer source documents and carries a punishment of up to three years or a fine. Section 66 addresses hacking and unauthorized data alteration, also carrying a maximum of three years or a fine. The statement suggesting a mandatory ten-year sentence for a first-time hacking offence is incorrect according to the Act's provisions.

**57.** (B) If it is essential in the national interest to intercept computer resource information.
The government has the power to instruct subscribers to assist in the interception or decryption of information under specific circumstances. This power is typically exercised when it is deemed essential in the interest of national security, public order, or the sovereignty and integrity of the country. In such cases, authorities can monitor or decrypt information transmitted through any computer resource.

**58.** (A) It applies to the execution of a Will under the Indian Succession Act, 1925.
The Information Technology Act 2000 has broad applicability across India and includes extraterritorial jurisdiction. It provides legal recognition for electronic records. However, there are specific legal documents that the Act does not cover. For instance, the execution of a Will under the Indian Succession Act, 1925, is explicitly excluded, meaning a Will cannot be legally executed in purely electronic form.

NODIA

**59.** (B) To ensure adequate integrity, security, and confidentiality of electronic records or payments.
The Central Government prescribes rules regarding the format and standards of Digital Signatures with a specific objective. These rules are designed to ensure the integrity, security, and confidentiality of electronic records and payments. By standardizing the digital authentication process, the government aims to prevent unauthorized tampering and to build a secure environment for digital commerce and e-governance throughout India.

**60.** (B) Physical theft of a banker's physical cash book.
Data theft under the Information Technology Act encompasses various digital offences, such as diminishing the value of electronic data or stealing source and object code. While Section 65 and Section 66 address these digital crimes, they do not cover physical theft. The physical theft of a banker's paper-based cash book would be prosecuted under traditional theft laws in the Indian Penal Code.

**61.** (C) P-2, Q-3, R-1, S-4
Digital Rights Management applications vary by content type. An e-book server typically restricts access, copying, and printing based on set constraints. Movie studio software often limits the number of copies a user can create. Company servers may be configured to block the forwarding of sensitive emails externally. Finally, music labels often include bits of information on CDs to confuse ripping software.

**62.** (C) Both (I) and (II)
The 2008 amendment to the Information Technology Act was comprehensive. It introduced Section 66A, which sought to penalize the sending of offensive messages, although this section was eventually declared unconstitutional by the Supreme Court. Additionally, the amendment introduced Section 69, which granted designated authorities the power to intercept, monitor, or decrypt information stored in or transmitted through any computer resource.

**63.** (A) P-4, Q-3, R-2, S-1
Specific computer crimes have defining characteristics and legal consequences. Introducing a virus involves executing instructions that spoil performance. Unauthorized access is addressed under Section 43, allowing for compensation. Data alteration is typically dealt with as hacking under Section 66. Lastly, publishing obscene information falls under Section 67, carrying a significant prison sentence for the first conviction and subsequent repeat offences.

**64.** (C) Only (I) and (II)
The Information Technology Rules of 2021 were designed to replace the 2011 Intermediary Guidelines. They mandate that digital portals and social media intermediaries must establish a clear grievance redressal procedure for users. However, significant social media intermediaries with more than five million users are not exempt; they are actually required to produce and publish detailed monthly compliance reports for transparency.

**65.** (A) 2008 Amendment - Penalties for child porn, cyber terrorism, and voyeurism
The 2008 Amendment to the Information Technology Act introduced several critical provisions to tackle modern cybercrimes. It established specific penalties for cyber terrorism, voyeurism, and child pornography, significantly strengthening the legal framework. Other options incorrectly associate different amendments with features like grievance redressal for OTT platforms, which were part of the 2021 rules, or the striking down of Section 66A.

**66.** (A) All (I), (II), (III), and (IV)
The Information Technology Act contains several key sections that define specific offences and authorities. Section 65 addresses tampering with computer source documents. Section 66 defines hacking and its associated punishments. Section 67 focuses on the publication of obscene electronic material. Finally, Section 68 outlines the authority of the Controller to issue orders, ensuring all listed statements correctly match the gist.

**67.** (III), (IV), (I), (II)
The chronological sequence of Information Technology legal milestones begins with the enactment of the original IT Act in 2000. This was followed by the 2008 Amendment, which introduced Sections 66A and 69. Subsequently,

Downloaded from www.pdf.tube

the 2012 Copyright Amendment enabled Digital Rights Management. Finally, the framing of the new IT Rules requiring grievance redressal for OTT platforms occurred most recently in 2021.

**68.** (A) Only (I)
When applying for a Digital Signature Certificate, it is a technical requirement that the applicant holds the private key corresponding to the public key to be listed in the certificate. Regarding procedural fairness, the Certifying Authority is indeed required to record its reasons in writing if an application for a certificate is rejected, ensuring that the decision-making process remains transparent and accountable.

**69.** (A) Only (I) and (III)
A computer contaminant is accurately defined as a set of instructions designed to modify, destroy, or record data. Such contaminants can also be used to usurp the normal operation of a computer system or network. Importantly, a contaminant does not need to be introduced physically via a USB drive; it can be transmitted electronically through networks, downloads, or email attachments.

**70.** (C) P-2, Q-1, R-4, S-3
In digital legal and technical terminology, a computer contaminant is code that modifies or destroys data. A Certifying Authority is the entity responsible for issuing Digital Signature Certificates. Meta tagging is a process used in Digital Rights Management prior to encryption to embed usage rules. Finally, the specific penalty for cyber terrorism was introduced to the Act via the 2008 amendment.

**71.** (A) All (I), (II), (III), and (IV)
The Information Technology Act includes several salient features. It elaborates on digital offences and penalties, defines cyber cafes as facilities for public internet access, and establishes the Cyber Regulations Advisory Committee. Furthermore, Section 81 provides that the Act's provisions generally have an overriding effect on other laws, ensuring a unified legal framework for the digital domain in India.

**72.** (B) P-3, Q-4, R-1, S-2
Each section of the Information Technology Act targets a specific legal area. Section 65 focuses on the tampering of computer source documents. Section 66 defines the crime of hacking. Section 68 details the Controller's authority to issue binding orders to ensure compliance. Finally, Section 71 establishes the penalty for misrepresentation, where individuals provide false information to obtain certificates or licenses.

**73.** (A) Only (I)
Under Section 67 of the Information Technology Act, sending pornographic or obscene emails is a punishable offence with significant imprisonment and fines upon first conviction. However, emails that contain threats of physical harm are not primarily addressed under Section 43 for compensation. Instead, such threatening communications are typically prosecuted as criminal intimidation under the relevant provisions of the Indian Penal Code.

**74.** (C) Decryption technology - Used to unlock content encrypted under DRM
Digital Rights Management relies on various technical concepts. Decryption technology is a fundamental component used to unlock digital content that has been secured via encryption. Conversely, meta tagging involves adding metadata, not removing it. A digital watermark is an embedded digital marker, not a physical stamp. Finally, peer-to-peer exchange is often what Digital Rights Management aims to restrict, rather than an endorsed mechanism.

**75.** (D) All (I), (II), (III), and (IV)
The Information Technology Act identifies several actions as computer crimes if performed without the permission of the owner. These include securing access to a network, downloading or extracting data, denying service to an authorized user, and manipulating a system to charge services to another person's account. All these actions represent unauthorized interference with computer resources and are subject to legal penalties.

**76.** (D) P-2, Q-4, R-1, S-3
Different digital legal concepts have distinct implications. The legal recognition of electronic records allows for the electronic maintenance of bank records. The acknowledgement of receipt can be confirmed by any conduct indicating receipt. Digital signatures validate authentication

NODIA

when affixed to a record. Finally, the submission of forms by electronic means facilitates modern e-banking through processes like online account opening.

**77.** (D) Only (I) and (II)
Under the Information Technology Act, any computer system or accessory that contravenes the rules is liable to be confiscated. The Act also empowers the government to investigate offences to maintain digital security. However, the authority to investigate cybercrimes is not limited to sub-inspectors; the Act specifies that a police officer not below the rank of Deputy Superintendent of Police should investigate.

**78.** (D) P-1, Q-2, R-3, S-4
Certain legal documents are excluded from the scope of the Information Technology Act. The Indian Succession Act applies to executing a Will, which is excluded. The Negotiable Instruments Act governs documents like cheques. The India Trust Act deals with the creation of trusts, and various property laws govern contracts for the sale of immovable property. All these documents must typically follow traditional non-electronic formats.

**79.** (B) Only (II)
The Information Technology Act specifies that any offence under its provisions should be investigated by a police officer not below the rank of Deputy Superintendent of Police. Regarding penalties, the Act clarifies that the imposition of a penalty or confiscation does not prevent the imposition of other punishments that a person may be liable for under any other existing laws or regulations.

**80.** (D) Reserve Bank of India Act, 1934 - Regulates the physical confiscation of computer floppy disks
The Information Technology Act 2000 impacted several statutes. The Indian Evidence Act now treats electronic records as documents, and the Banker's Book of Evidence Act includes electronic data printouts. The Indian Penal Code covers defamatory emails. However, the Reserve Bank of India Act does not regulate the physical confiscation of computer equipment; such confiscation is governed by Section 76 of the IT Act.

**81.** (C) Only (I), (II), and (III)
Digital Rights Management relies on several core concepts to protect digital content. These include using encryption and digital watermarks for secure distribution, controlling content exploitation through the use of meta tagging, and enforcing license rights that are established before the content is encrypted. Section 66A is not a component of Digital Rights Management, as it was a penal provision for offensive messages.

**82.** (B) Only (I) and (II)
For the retention of electronic records to be legally valid, two main conditions must be satisfied. First, the information must remain accessible so it can be used for subsequent reference. Second, the record must be retained in the original format in which it was generated, sent, or received. There is no legal requirement to print and physically file these electronic records for validity.

**83.** (B) Only (I), (II), and (III)
The rules for the acknowledgement of receipt of electronic records specify that if an originator requests it, the receipt must be acknowledged. In the absence of an agreed method, any communication or conduct by the addressee indicating that the record was received is legally sufficient. There is no requirement for the acknowledgement itself to be digitally signed by a Certifying Authority for validity.

**84.** (C) Only (I) and (II)
Specific cyber offences are categorized under different sections of the Information Technology Act. Hacking into a computer system falls under Section 66. Similarly, if the introduction of malicious code or a contaminant results in data loss, Section 66 is applied alongside Section 43. Denial of Service is also an offence under the Information Technology Act, rather than being exclusively penalized by the IPC.

**85.** (A) Only (I)
When verifying a digital signature, a court has the power to direct the Controller or the Certifying Authority to produce the Digital Signature Certificate. Furthermore, the court is legally permitted to direct any other person to apply the public key listed in the certificate. This process allows the court to verify whether the

Click Here to Buy book on Amazon

digital signature was indeed affixed by the person claimed.

**86.** (B) P-2, Q-4, R-3, S-1
The Information Technology Act provided various benefits through legislative amendments. The Indian Penal Code now covers defamatory emails under Section 500. The Indian Evidence Act treats electronic records as admissible documents for court inspection. The Banker's Book of Evidence Act allows printouts of electromagnetic data to be used as business books. Conversely, the Negotiable Instruments Act remains largely excluded from these digital provisions.

**87.** (A) P-4, Q-3, R-1, S-2
Penalties under the Information Technology Act are tailored to the offence. Section 70 subjects individuals to imprisonment and fines for violating protected system access. Section 71 punishes misrepresentation with two years in prison and a fine of one lakh rupees. Section 74 imposes a penalty of up to two years or a fine for fraudulent publication. Lastly, Section 43 provides for compensation up to one crore rupees.

**88.** (B) P-1, Q-2, R-3, S-4
Legal issues in the digital space map to specific provisions. Data theft is typically addressed as hacking under Section 66 of the Information Technology Act. Defamatory emails are prosecuted under Section 500 of the Indian Penal Code. The breach of confidentiality and privacy is penalized under Section 72 of the IT Act. Finally, interception for national interest is carried out under the authority of Section 69.

**89.** (D) P-2, Q-3, R-1, S-4
Each component of Digital Rights Management serves a specific function. Encryption locks content, requiring decryption to unlock. Digital watermarks are embedded markers used to track ownership. Secure distribution is the general mechanism used to track and protect content from unauthorized copying. Finally, license rights consist of usage rules that define exactly how a consumer is permitted to exploit the purchased digital content.

**90.** (A) Section 72 - Controller's authority to issue orders
The pairing of Section 72 with the Controller's authority to issue orders is incorrect. Section 72 actually deals with the penalty for the breach of confidentiality and privacy. The Controller's authority to issue specific orders for compliance is found under Section 68 of the Information Technology Act. Other pairings, such as Section 65 for tampering and Section 67 for obscenity, are correctly identified.

**91.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Banks must ensure their computer systems are used solely for authorized banking business to maintain security and compliance. This is critical because, under the Information Technology Act, any computer system or accessory involved in a contravention of the Act is liable to confiscation. Therefore, preventing unauthorized use is essential to protect the bank's operational infrastructure from being legally seized by authorities.

**92.** (C) Computer Crime by downloading data without authorization from the owner.
When an employee downloads a customer database without the permission of the owner or person in charge, they have committed a computer crime. Under the Information Technology Act, downloading, copying, or extracting data from a computer system without authorization is a prohibited act. Such actions compromise data security and privacy, leading to potential civil liabilities for compensation and criminal penalties for hacking.

**93.** (C) Only (I), (II), (III), and (IV)
The Information Technology Act defines specific imprisonment terms for various offences. Tampering with source documents carries up to three years. Publishing obscene information is punishable with up to five years for the first conviction and ten years for subsequent convictions. Misrepresentation carries a penalty of up to two years. However, the failure to comply with a controller's orders results in up to three years, not five.

Downloaded from www.pdf.tube

**94.** (C) 3 years
Hacking into a computer system and altering transaction data are serious offences under Section 66 of the Information Technology Act. Regardless of the underlying motive, such as covering up embezzlement, the unauthorized alteration of data is legally categorized as hacking. The maximum recommended prison term for an individual found guilty of this offence under the Act is three years, often accompanied by a fine.

**95.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
The Information Technology Act 2000 is characterized by its extraterritorial jurisdiction. This means the Act applies to any person who commits an offence or contravention, regardless of their nationality or physical location. The critical factor for jurisdiction is whether the act involves a computer, computer system, or computer network located within the territory of India, allowing for the prosecution of global offenders.

**96.** (B) Section 70
Section 70 of the Information Technology Act deals specifically with "protected systems." These are computer resources that the appropriate government designates through official notification. Any individual who secures or attempts to secure unauthorized access to such a declared protected system is in violation of this specific section and is subject to severe penalties, including imprisonment for up to ten years and fines.

**97.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Banks are encouraged to replace bulky physical records with electronic systems due to legislative changes. The Indian Evidence Act was amended to recognize electronic records and printouts of electromagnetically stored data as legal documents. This modernization allows banks to maintain digital records that are legally valid for court inspection, thereby improving efficiency and reducing the physical space required for traditional record-keeping.

**98.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Within the framework of the Information Technology Act, internal bank authentication can be legally satisfied through the use of Digital Signatures. The Act provides that where any law requires a signature, that requirement is fulfilled if the information is authenticated by a digital signature. These signatures must be affixed in a manner and format as prescribed by the Central Government's specific rules.

**99.** (B) Yes, due to amendments allowing electromagnetically stored data as evidence.
In a court case, a bank's submission of a printout from a ledger stored on an electromagnetic tape drive is legally recognized. This recognition is due to amendments in the Bankers' Books Evidence Act and the Indian Evidence Act. These changes ensure that data stored on electronic media and their certified printouts are treated as admissible evidence, just like traditional paper-based business books.

**100.** (D) Assertion (A) is false, but Reason (R) is true.
Section 66A of the Information Technology Act does not actively penalize offensive messages today because it was struck down by the Supreme Court. The court ruled that the section was unconstitutional because it arbitrarily and disproportionately invaded the fundamental right to free speech guaranteed under Article 19(1). While the reasoning for the court's decision is true, the assertion of its continued enforcement is false.

NODIA

**101.** (A) Digital Rights Management (DRM)
Configuring servers to block the forwarding of sensitive emails externally is a practical application of Digital Rights Management technology. Digital Rights Management systems are designed to control and restrict the usage and redistribution of digital content according to predefined rules. By preventing the unauthorized dissemination of sensitive information, the corporation is using Digital Rights Management to protect its internal intellectual property and maintain confidentiality.

**102.** (A) All (I), (II), (III), and (IV) and (V)
The Information Technology Act 2000 contains specific exemptions regarding its applicability. It does not apply to negotiable instruments, powers of attorney, trusts, wills, or contracts for the sale of immovable property. All these documents are explicitly excluded from the digital recognition framework provided by the Act. Therefore, they must generally be executed using traditional paper-based methods rather than solely electronic records or signatures.

**103.** (B) That the subscriber holds the private key matching the public key in the pair.
When a bank acts as a Certifying Authority, a System Auditor must verify technical compliance regarding key pairs. A fundamental requirement for issuing a Digital Signature Certificate is ensuring that the subscriber holds the private key that corresponds to the public key listed in the certificate. This verification is essential to maintain the security and integrity of the digital signature authentication process.

**104.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
System Auditors play a vital role when banks function as Certifying Authorities. They are responsible for verifying that the process for issuing Digital Signature Certificates complies with the legal requirements. The Reason correctly explains this role, as the auditor must ensure the bank follows all provisions of the Information Technology Act, rules, and regulations to maintain the integrity of the digital certificates.

**105.** (C) Three years in jail and a fine.
Under Section 68 of the Information Technology Act, the Controller has the authority to issue orders to Certifying Authorities or their employees to ensure compliance. If an entity, such as an Internet Service Provider, refuses to comply with these official orders, it constitutes a criminal offence. The prescribed penalty for such non-compliance is imprisonment for up to three years and a fine.

**106.** (B) Only (I), (II), (III), and (IV)
The Information Technology Act defines several offences, including hacking, misrepresentation to a Certifying Authority, breach of confidentiality, and publication for a fraudulent purpose. Each of these acts results in a penalty or equipment confiscation. Conversely, legally retaining an electronic record for subsequent reference is a compliant action authorized by the Act, rather than an offence that would result in a legal penalty.

**107.** (A) IPC provisions pertaining to criminal intimidation and physical threats.
While the Information Technology Act covers many cybercrimes, emails containing threats of physical harm are primarily addressed by the Indian Penal Code. Specifically, provisions related to criminal intimidation are applied to such communications. Defamation and obscenity are handled under different sections, and Section 66A has been struck down, leaving the Indian Penal Code as the primary framework for prosecuting threats of physical violence.

**108.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
If the introduction of malicious code leads to data loss, both Section 43 and Section 66 of the Information Technology Act become applicable. Section 43 focuses on the civil aspect, allowing the victim to seek compensation for the damage. Section 66 provides the criminal framework for prosecuting the unauthorized alteration and hacking of data, ensuring both financial recovery and penal consequences.

**109.** (D) Misrepresentation, which is considered a committed computer crime.
Suppressing material facts or providing false information while applying for a license or certificate is classified as misrepresentation. Under Section 71 of the Information Technology Act, this action is recognized as a committed computer crime. The law penalizes such acts to ensure that Certifying Authorities and the Controller operate based on truthful information, maintaining the overall trustworthiness of the digital authentication framework.

**110.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
The Information Technology Act 2000 is designed to provide a comprehensive framework for the

Click Here to Buy book on Amazon

# CHAPTER 14
# Emerging Technologies

Oct/Nov 2006

**1.** What is the primary function of an API Banking Platform in the modern financial technology landscape?
(A) To eliminate the need for back-office operations in traditional banking.
(B) To mandate a centralized government portal for all financial transactions.
(C) To permanently replace human customer service with virtual bot systems.
(D) To bridge bank backend operations and third-party frontend experiences.

May/June 2015

**2.** Consider the following statements regarding types of blockchains:
I A public blockchain requires a large amount of computational power and offers little or no transaction privacy.
II A private blockchain is decentralized but governed by a single organization that controls who is authorized to participate.
III A consortium blockchain is suited for commercial situations where all parties share responsibility for the blockchain.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

Oct/Nov 2021

**3.** Which of the following statements accurately describes the operational model of Neo or Digital Banks?
(A) They need to maintain a set number of physical brick-and-mortar locations.
(B) They increase the operational expenses of all currently active banks.
(C) They offer digital banking services without requiring physical branches.
(D) They use decentralized blockchain networks for all internal accounting.

NODIA

May/June 2008

**4.** What is the most appropriate application of predictive analytics in the commercial sector?
(A) Executing physical cash transfers between bank branches.
(B) Encrypting databases to protect against ransomware attacks.
(C) Analyzing digital marketing data to observe changes in consumer behavior.
(D) Designing physical layouts for neo-bank branches and offices.

Oct/Nov 2014

**5.** Which of the following statements correctly describes Semi-structured data in the context of Big Data Analytics?
(A) Data that is highly organized and exists in a fixed format, such as a CSV file.
(B) Data containing keywords that can be used for identification and processing.
(C) Data that has no clear format and is impossible to parse for financial modeling.
(D) Data that exists purely as encrypted binary code on a blockchain network.

May/June 2011

**6.** Match the components of Artificial Intelligence in banking (List I) with their descriptions (List II):
List I: (Component)
P. Fraud detection
Q. Meeting regulatory requirements
R. Lowering costs
S. Improving the customer experience
List II: (Description)
1. Automating the frontline and utilizing customer-facing virtual assistants.
2. Deriving deep actionable insights for faster decision making based on behaviour patterns.
3. Identifying suspicious behaviour while it is happening using location data.
4. Monitoring data on a real-time basis to flag compliance issues sooner.

of trust between the bank and its customers in the digital age.

**119.** (A) A Computer Crime, as creating or publishing a DSC for fraudulent purpose.
The creation or publication of a forged Digital Signature Certificate for a fraudulent purpose, such as securing a loan, is explicitly classified as a computer crime. Under the Information Technology Act, specifically Section 74, such actions are heavily penalized. This protection is necessary to ensure the reliability of digital certificates, which are essential for authenticating identities and transactions in the electronic environment.

**120.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
The Information Technology Act 2000 possesses extraterritorial jurisdiction, allowing for the prosecution of individuals regardless of their location or nationality. The primary condition for this jurisdiction is that the offence or contravention must involve a computer resource that is physically located within India. This ensures that the Indian legal system can address cybercrimes targeted at its infrastructure from anywhere in the world.

**121.** (D) No, the Act does not apply to a power of execution of an attorney.
Although the Information Technology Act provides broad legal recognition for electronic records, certain legal documents are explicitly excluded from its applicability. One such exclusion is a power of execution of an attorney. Therefore, an individual cannot legally execute a Power of Attorney solely through electronic means under the current provisions of the Act, regardless of their residency status or the type of transaction.

**122.** (C) The enforcement of license rights and usage rules on the content.
When a consumer is restricted from printing a purchased e-book, it demonstrates the enforcement of Digital Rights Management license rights. These rights are usage rules embedded into the digital file's metadata before encryption. When the user attempts an action like printing, the software checks the permitted rules. If the license does not allow printing, the system blocks the action to prevent unauthorized exploitation.

**123.** (C) Yes, the Act has extraterritorial jurisdiction for systems located in India.
A foreign national can be prosecuted under the Information Technology Act for hacking into a server located in India. This is possible because the Act includes extraterritorial jurisdiction. The law applies to any person, regardless of their nationality or location, if their unauthorized actions involve a computer, computer system, or computer network that is situated within the sovereign territory of India.

**124.** (A) The Information Technology (IT) Rules, 2021.
A social media platform with millions of users that fails to publish required monthly compliance reports is in violation of the Information Technology Rules, 2021. These rules specifically mandate that significant social media intermediaries must provide transparency by detailing user complaints and actions taken. This framework was established to increase the accountability of large digital platforms operating within the Indian digital ecosystem.

**125.** (B) No, the Act is not applicable to contracts for the sale of immovable property.
Contracts for the sale of immovable property, or any interest in such property, are explicitly excluded from the applicability of the Information Technology Act 2000. Because of this exclusion, such contracts cannot be legally executed or recognized as valid through purely electronic means under this specific Act. They must follow traditional legal procedures and documentation formats as required by relevant property and registration laws.

www.nodia.in

Downloaded from www.pdf.tube

digital domain. Section 81 of the Act explicitly states that its provisions shall have an overriding effect notwithstanding anything inconsistent contained in any other law for the time being in force. This ensure that digital transactions and offences are governed primarily by this specialized legislation when conflicts arise.

**111.** (D) Deputy Superintendent of Police
To ensure that complex digital crimes are handled with appropriate expertise, the Information Technology Act specifies the rank of investigating officers. It mandates that no police officer below the rank of Deputy Superintendent of Police shall investigate any offence committed under the Act. This requirement helps maintain a high standard of investigation for sophisticated cyber frauds and other technical digital offences.

**112.** (B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
Digital Rights Management products were indeed developed to counter the rise of online piracy and peer-to-peer sharing. Additionally, the primary aim of Digital Rights Management is to restrict unauthorized redistribution and control how consumers copy content. While both statements accurately describe the context and goal of Digital Rights Management, the second statement describes its function rather than explaining why the technology was originally developed.

**113.** (C) Assertion (A) is true, but Reason (R) is false.
India's copyright law was amended in 2012 to include Digital Rights Management provisions, aligning it with international standards for digital media protection. This makes the assertion true. However, the reason provided is false because India is a signatory to the World Intellectual Property Organization Copyright Treaty, having acceded to it in 2018 to align its domestic legal framework for content protection with international standards.

**114.** (B) Section 65
Section 65 of the Information Technology Act specifically addresses the theft or tampering of computer source documents. This includes the intentional concealment, destruction, or alteration of computer source code. Because source code is the foundational intellectual property of software, its protection is vital. Any individual who unauthorizedly interferes with this code is subject to imprisonment for up to three years or a fine.

**115.** (D) The Act does not grant the right to insist on electronic monetary transactions.
While the Information Technology Act promotes the use of electronic records, it contains a specific limitation regarding their mandatory use. The Act clarifies that its provisions do not confer any legal right upon a person to insist that any organization must accept documents or monetary payments in electronic form. Therefore, a bank can choose whether to accept electronic payments based on its own policies.

**116.** (D) Only (I), (II), (III), and (IV)
Digital Rights Management is practically applied through various technical restrictions on digital content. These include blocking the forwarding of sensitive emails, restricting the printing of e-books, limiting the number of copies made by DVD software, and adding data to CDs to confuse ripping programs. Publishing lists of cybercriminals in newspapers is a public disclosure measure and does not involve technical content protection mechanisms.

**117.** (D) Section 43 and Section 66.
When a cybercriminal introduces a Trojan that results in massive data deletion, multiple sections of the Information Technology Act apply. Section 43 is used to address the civil liability and compensation for the damage caused to the computer system. Simultaneously, Section 66 is invoked for criminal prosecution regarding the unauthorized alteration, destruction, or hacking of the financial data contained within the system.

NODIA

**118.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Disclosing electronic records without authorization is a computer crime because it violates the fundamental principles of privacy and confidentiality. For bankers, this is particularly critical as they handle sensitive customer account details. Since maintaining customer secrecy is a paramount legal obligation, any unauthorized disclosure is penalized to protect the relationship

(A) P-1, Q-2, R-3, S-4
(B) P-3, Q-4, R-1, S-2
(C) P-4, Q-3, R-2, S-1
(D) P-2, Q-1, R-4, S-3

**Oct/Nov 2010**

**7.** The total digital transaction volume in the annual report 2020-21 of the Reserve Bank of India has risen by what percentage against the previous year?
(A) 15%
(B) 20%
(C) 28%
(D) 35%

**May/June 2019**

**8.** Match the Big Data analytics categories (List I) with their typical outcomes in the banking industry (List II):
List I: (Big Data Analytics Category)
P. Enhanced Fraud Detection
Q. Superior Risk Assessment
R. Increased Customer Retention
S. Product Personalization
List II: (Outcome)
1. Developing long-lasting customer interactions based on detailed client profiles.
2. Raising red lights on risky client profiles using predictive capabilities.
3. Creating products and offerings suited to specific needs based on existing profiles.
4. Tracking transactional activities on an individual level to build secure consumer profiles.
(A) P-2, Q-3, R-4, S-1
(B) P-4, Q-2, R-1, S-3
(C) P-1, Q-4, R-3, S-2
(D) P-3, Q-1, R-2, S-4

**Oct/Nov 2024**

**9.** Which of the following pairs concerning Blockchain types is incorrect?
(A) Public Blockchain - Bitcoin
(B) Consortium Blockchain - Governed exclusively by a single organization
(C) Private Blockchain - Hosted on company premises behind a firewall
(D) Distributed Ledger System - Immutable database structure

**May/June 2021**

**10.** Which of the following pairs correctly matches the open banking concept with its direct consumer benefit?
(A) Better payment options - Eradicating interest on corporate loans.
(B) Better borrowing terms - Generating returns on high-risk equity.
(C) Account aggregation - Consolidating all accounts into one view.
(D) Better financial management - Converting fiat into cryptocurrency.

**Oct/Nov 2007**

**11.** Consider the following statements regarding AI, ML, and Cognitive Computing:
I Artificial Intelligence is built upon the concept of Machine Learning.
II Cognitive Computing covers disciplines including machine learning, NLP, vision, and human-computer interaction.
III Artificial Intelligence is entirely independent of Machine Learning and Cognitive Computing.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

**May/June 2024**

**12.** Which of the following statements regarding the parties involved in Open Banking is incorrect?
(A) Financial service providers will be able to dramatically innovate on their product offers to businesses.
(B) Enterprises will benefit from more effective and efficient financial instruments, resulting in greater automation.
(C) Central banks act as the exclusive data aggregators and intermediaries for all open banking transactions.
(D) Customers will benefit from improved ways to spend, borrow, and invest as a result of open banking.

**Oct/Nov 2018**

**13.** Why does a blockchain create a trusted record of transactions that is resistant to data tampering?
(A) It links blocks via cryptographic hashes of previous data to ensure immutability.
(B) It stores data in a centralized database

Click Here to Buy book on Amazon

controlled by a single government authority.
(C) It records transactions only after they are manually verified by an external auditor.
(D) It automatically deletes old blocks periodically to prevent sophisticated hacking attempts.

May/June 2014

**14.** Which of the following is an incorrect statement regarding the major benefits of leveraging Big Data Analytics in banking?
(A) It allows banks to create consumer profiles to track transactional activities on an individual level for enhanced fraud detection.
(B) It raises red lights on client profiles that are riskier when integrated into business intelligence systems.
(C) It standardizes product offerings so that all unique customers receive the exact same generic services.
(D) It helps to sort through feedback and respond in a timely manner, streamlining customer feedback.

Oct/Nov 2012

**15.** Which statement correctly identifies a principal benefit of utilizing cognitive analytics over traditional big data analytics?
(A) It requires extensive manual tagging with metadata before datasets can be fed into a computer.
(B) It relies exclusively on structured data formatted in CSV files for financial report generation.
(C) It completely replaces the need for any machine learning algorithms in the analysis phase.
(D) It allows for the processing of large, unstructured datasets without pre-tagging.

May/June 2007

**16.** What is the core convergence goal of technologies such as artificial intelligence, internet of things, voice banking, and banking as a service?
(A) Invisible banking
(B) Eliminating cyber threats
(C) Mandatory blockchain adoption
(D) Eradicating physical currencies

NODIA

Oct/Nov 2022

**17.** How is Artificial Intelligence formally defined in the field of computer science?
(A) The engineering of intelligent machines and computer programs.
(B) The physical manufacturing of robotic hardware for assembly lines.
(C) The migration of banking operations to cloud computing environments.
(D) The statistical modeling of financial data using manual entry systems.

May/June 2020

**18.** Match the following Embedded Finance models (List I) with their corresponding characteristics (List II):
List I: (Embedded Finance Model)
P. Embedded Payments
Q. Embedded Card Payments
R. Embedded Lending
S. Embedded Investments
List II: (Characteristics)
1. Allowing users to apply for and receive a loan at the point of purchase without third-party involvement.
2. Faster checkout and settlement processes from a single location without digging for cash.
3. Streamlining the process by providing users a centralized platform for the stock market and mutual funds.
4. Transferring funds electronically to a virtual or smart medium for secure, encrypted purchases.
(A) P-2, Q-4, R-1, S-3
(B) P-1, Q-3, R-2, S-4
(C) P-4, Q-1, R-3, S-2
(D) P-3, Q-2, R-4, S-1

Oct/Nov 2013

**19.** Which of the following statements incorrectly identifies a use case of Blockchain in Banking?
(A) It accelerates international transfers by enabling faster peer-to-peer transactions.
(B) It lowers costs by automating tasks like payments or the issuance of loans.
(C) It aids in fraud prevention by creating a visible audit trail with redundancies.
(D) It increases human error by requiring complex manual record-keeping processes.

May/June 2005

**20.** What is the most appropriate strategic advantage a bank gains from Big Data analysis concerning regulatory obligations?
(A) It streamlines compliance verification, auditing, and reporting processes.
(B) It allows the bank to bypass standard regulatory audits and inspections.
(C) It automates the drafting of all new national banking laws and rules.
(D) It restricts customers from submitting feedback on social media networks.

Oct/Nov 2015

**21.** Consider the following statements regarding Machine Learning (ML):
I ML algorithms learn from data and create foresights without being explicitly programmed.
II ML is primarily used for tasks where designing explicit algorithms with good performance is easy and highly feasible.
Which of the above statement(s) is/are correct?
(A) Only (I) is correct
(B) Only (II) is correct
(C) Both (I) and (II) are correct
(D) Neither (I) nor (II) is correct

May/June 2025

**22.** Which of the following is NOT listed as a core emerging technology currently influencing the Banking and Financial Sector?
(A) Robotic Process Automation
(B) Electromagnetic Telegraphy
(C) Cyber Security - Zero Trust Security model
(D) Block chain

Oct/Nov 2009

**23.** How do embedded investments streamline the investment process for users?
(A) By transferring funds automatically to offshore tax haven locations.
(B) By forcing users to physically visit brokerage firms for confirmations.
(C) By bypassing all regulatory compliance required for market investments.
(D) By offering a platform for investing without leaving the current site.

May/June 2017

**24.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): Blockchain eliminates the risk of tampering by a malicious actor and creates a trusted record of transactions.
Reason (R): Each successive block reinforces the prior block's verification, making the irreversible chain tamper-evident.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Oct/Nov 2025

**25.** Consider the following statements regarding the mechanics of Blockchain:
I The timestamp validates that the transaction data existed at the time the block was released.
II Blocks can be easily edited or inserted between two existing blocks to update records.
Which of the above statement(s) is/are correct?
(A) Only (I) is correct
(B) Only (II) is correct
(C) Both (I) and (II) are correct
(D) Neither (I) nor (II) is correct

May/June 2012

**26.** How is Open Banking formally defined within the financial technology ecosystem?
(A) A framework where core banking systems are migrated to public cloud servers.
(B) A regulatory sandbox allowing fintechs to bypass all compliance mandates.
(C) A decentralized ledger system eliminating any central banking authority.
(D) A system for sharing data with user consent to provide financial services.

Oct/Nov 2020

**27.** Arrange the following AI application domains in the progressive order from foundational automation to complex insight extraction, as categorized in the finance industry:
I Cognitive insight
II Cognitive automation
III Cognitive engagement

NODIA

monetary policy.
(B) CBDC is freely convertible against commercial bank money and cash.
(C) CBDC appears as an asset on the central bank's balance sheet.
(D) CBDC is a fungible legal tender for which holders need not have a bank account.

**Oct/Nov 2014**

**86.** Why do banking sector applications heavily prefer private clouds over public clouds for mission-critical workloads?
(A) Private clouds offer greater economies of scale and higher ROI.
(B) Private clouds provide increased security to ensure data is not misplaced or lost.
(C) Public clouds completely restrict access to API integrations.
(D) Public clouds lack any form of disaster recovery plans.

**May/June 2012**

**87.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): It is essential for CBDCs to implement post-quantum, quantum-secure cryptographic algorithms.
Reason (R): Quantum computers possess processing power that far outstrips current supercomputers, capable of fending off traditional encryption methods.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2025**

**88.** What is the most appropriate primary objective of deploying Digital Banking Units (DBUs) across the country?
(A) To replace all physical currency with private cryptocurrencies.
(B) To improve financial inclusion and management transparency.
(C) To centralize all corporate lending processes in a single location.
(D) To reduce costs by entirely eliminating customer service.

**May/June 2024**

**89.** Match the Form of CBDC (List I) with its core characteristic (List II):
List I: (Form of CBDC)
P. Token-based CBDC
Q. Account-based CBDC
R. Bearer-instrument
S. Identity verification
List II: (Characteristic)
1. Whosoever holds it at a given point in time is presumed to own it.
2. Preferred mode for CBDC-W, requiring maintenance of record of balances.
3. Characteristic of token-based CBDC where the receiver verifies the token is genuine.
4. Required in an account-based system, performed by an intermediary.
(A) P-2, Q-1, R-4, S-3
(B) P-1, Q-2, R-3, S-4
(C) P-3, Q-4, R-1, S-2
(D) P-4, Q-3, R-2, S-1

**Oct/Nov 2018**

**90.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): Central Bank Digital Currencies (CBDCs) serve as a liability of the issuing central bank.
Reason (R): CBDCs are essentially a new variant of central bank money denominated in an existing unit of account, functioning as legal tender.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2014**

**91.** Which of the following is NOT one of the three primary classifications of Big Data?
(A) Structured
(B) Macro-structured
(C) Unstructured

Downloaded from www.pdf.tube

# STUDYING FROM PDFs?

# THINK AGAIN.

If you are studying only from PDFs,
you are wasting valuable time.

Research shows that learning from

**PRINTED BOOKS** has up to

**4× HIGHER RETENTION**

than studying from screens.

**PRINT BOOK = BETTER MEMORY**

**PDF = LOWER RETENTION**

Those who study from **PRINTED BOOKS**
move **AHEAD.**

Others are left **BEHIND**
in competition.

In competitive exams,
being average is not enough.

## STAY ONE STEP AHEAD.

May/June 2018

**36.** Identify the correct pair regarding the predicted technology adoption in the Financial Services Industry Worldwide (Sep 2020).
(A) Cloud Computing - 55%
(B) AI - 62%
(C) Big Data Analytics - 91%
(D) AR/VR - 98%

Oct/Nov 2011

**37.** Consider the following statements regarding Robotic Process Automation (RPA):
I RPA software is geared towards automating mundane, repetitive, rule-based processes.
II RPA implementation allows accounting staff to devote more time to serving clients and higher-value work.
III RPA operates at the individual data field level across banking software platforms for seamless operation.
IV RPA requires constant human intervention to copy-paste information from one banking system to another.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (III)
(B) (II), (III), and (IV)
(C) (I), (III), and (IV)
(D) (I), (II), and (IV)

May/June 2022

**38.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): Zero Trust Architecture (ZTA) is highly effective in mitigating successful cyber security incidents caused by uninhibited lateral movement.
Reason (R): ZTA authenticates and authorizes actors only at the perimeter level and leaves internal network movements unmonitored.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Oct/Nov 2023

**39.** Consider the following statements about the 5G Network:
I 5G is the fifth generation of cellular network based on OFDM principles.
II 5G latency times are typically less than 1 millisecond.
III 5G is roughly ten to one hundred times faster than 4G.
IV 5G operates exclusively on sub-2 GHz bandwidths to prevent interference.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (III)
(B) (II), (III), and (IV)
(C) (I), (III), and (IV)
(D) (I), (II), and (IV)

May/June 2009

**40.** To fuel its AI mission, State Bank of India launched a national hackathon to invite developers and startups to create innovative solutions. What was the name of this hackathon?
(A) “Hack the Bank”
(B) “AI for Finance”
(C) “Digital India Codefest”
(D) “Code For Bank”

Oct/Nov 2005

**41.** Which of the following is an incorrect pair regarding the four core Fintech areas?
(A) Digital lending - Facilitating quick credit
(B) Digital wealth management - Manual paper-based ledger storage
(C) Payments - Streamlining financial transactions
(D) Blockchain - Housing encrypted transactions

May/June 2010

**42.** Consider the following statements about the use cases of RPA in banking:
I Extracting required information to auto-fill Suspicious Activity Reports (SARs).
II Gathering data from KYC documents using Optical Character Recognition (OCR) for customer on-boarding.
III Providing high-level advisory on complex personal wealth management portfolios.
IV Eliminating data transcription errors in the account opening process.
V Facilitating critical mortgage lending processes like financial comparisons and quality control.

NODIA

(A) (I), (II), (III)
(B) (II), (III), (I)
(C) (III), (I), (II)
(D) (II), (I), (III)

**May/June 2006**

**28.** What does the term "embedded banking" or "embedded finance" represent?
(A) The use of financial instruments or services by a non-financial supplier.
(B) The physical placement of ATM machines inside retail shopping malls.
(C) The mandatory integration of banking apps with government taxation platforms.
(D) The conversion of physical bank branches into digital-only self-service kiosks.

**Oct/Nov 2017**

**29.** Which of the following is NOT an inherent limitation of Blockchain technology?
(A) Scalability constraints due to limited transactions processed per second.
(B) Storage issues as the database grows with the number of transactions.
(C) The ease of reversing transactions without the consent of network nodes.
(D) Privacy concerns since data on a public blockchain is accessible to nodes.

**May/June 2016**

**30.** When banks create a 360-degree image of their consumers by combining personal and transactional data, which of the following is NOT typically a resulting action?
(A) Keeping track of customer spending habits.
(B) Segmenting customers depending on their profiles.
(C) Customizing product offerings.
(D) Deleting legacy customer data to free up server storage.

**Oct/Nov 2008**

**31.** Which of the following is an exception to the processes typically automated using RPA in banks?
(A) Anti-Money Laundering (AML)
(B) Opening a bank account
(C) Conducting emotional intelligence assessments of bank employees
(D) Lending on mortgages

**May/June 2023**

**32.** Which of the following is an incorrect statement regarding the basic tenets of Zero Trust Architecture?
(A) No resource is inherently trusted, and every asset must have its security posture evaluated.
(B) Devices on the network must be owned and configurable exclusively by the enterprise.
(C) Not all enterprise resources are on enterprise-owned infrastructure.
(D) Assets and workflows moving between enterprise and nonenterprise infrastructure should have a consistent security policy.

**Oct/Nov 2019**

**33.** By accelerating loan processing using RPA, banks have brought the processing time down to a record of how many minutes?
(A) 1-5 minutes
(B) 5-10 minutes
(C) 10-15 minutes
(D) 20-25 minutes

**May/June 2013**

**34.** How will 5G enable banks to deploy "mobile pop-up branches"?
(A) By utilizing legacy 3G networks to stream low-bandwidth text data.
(B) By mandating customers to physically carry personal servers to remote locations.
(C) By replacing all mobile applications with SMS-based banking.
(D) By using portable mobile banks to deliver VR experiences.

**Oct/Nov 2016**

**35.** Consider the following statements about ICICI Bank's software robotics:
I The software robots have increased the response time to customers by up to 60 percent.
II The software robots have increased accuracy to 100 percent, sharply improving productivity.
Which of the above statement(s) is/are correct?
(A) Only (I) is correct
(B) Only (II) is correct
(C) Both (I) and (II) are correct
(D) Neither (I) nor (II) is correct

Click Here to Buy book on Amazon

connect to its systems before granting access.
III It promotes granting users the maximum amount of access by default.
IV It encourages micro-segmentation of internal networks into smaller VLANs.
V It relies entirely on a single perimeter firewall to secure all data.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (IV)
(B) (II), (III), and (V)
(C) (I), (III), and (IV)
(D) (I), (II), and (V)

**Oct/Nov 2023**

**51.** Consider the following statements regarding the definition of Fintech:
I It involves technology-enabled innovation in financial services.
II It is strictly limited to innovations that have absolutely no material effect on the provision of financial services.
Which of the above statement(s) is/are correct?
(A) Only (I) is correct
(B) Only (II) is correct
(C) Both (I) and (II) are correct
(D) Neither (I) nor (II) is correct

**May/June 2012**

**52.** How does RPA achieve "zero infrastructure cost" in financial services?
(A) By replacing all physical branch networks with virtual realities.
(B) By forcing cloud providers to waive all hosting fees.
(C) By converting all fiat transactions into decentralized cryptocurrency.
(D) By using UI automation to work within existing legacy systems.

**Oct/Nov 2025**

**53.** Match the Indian bank (List I) with its corresponding AI initiative (List II):
List I: (Indian Bank)
P. SBI
Q. HDFC Bank
R. ICICI Bank
S. Axis Bank
List II: (AI Initiative)
1. Deployed software robotics in over 200 business processes to emulate human actions.
2. Launched an AI & NLP enabled app for Conversational Banking to answer FAQs 24x7.
3. Created an Electronic Virtual Assistant (EVA) for faster customer service.
4. Launched a national hackathon focusing on predictive analytics, Fintech, and BOTS.
(A) P-1, Q-2, R-3, S-4
(B) P-3, Q-4, R-2, S-1
(C) P-4, Q-3, R-1, S-2
(D) P-2, Q-1, R-4, S-3

**May/June 2022**

**54.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): The deployment of 5G will vastly expand the opportunities for the Internet of Things (IoT) in the banking sector.
Reason (R): 5G offers far lower latency and improved connectivity, allowing more smart gadgets to connect and interact in real-time.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2011**

**55.** In the context of Zero Trust Architecture, how should the enterprise private network be perceived?
(A) As an environment where an attacker is assumed to be constantly present.
(B) As a universally safe zone requiring no internal encryption of sensitive data.
(C) As an implicit trust zone where assets are free from external or internal attack.
(D) As a hardware-only environment where software verification is entirely redundant.

**May/June 2018**

**56.** Which of the following is an incorrect statement regarding the benefits of RPA?
(A) RPA implementation requires significant changes in infrastructure due to a lack of UI automation capabilities.
(B) RPA provides a drag and drop technology to

NODIA

automate workflows with minimal coding requirements.
(C) RPA robots work 24x7 to complete tasks, ensuring ever-present availability.
(D) RPA helps in generating full audit trails for processes to reduce business risk.

**Oct/Nov 2017**

**57.** Which statement accurately highlights a major drawback or challenge of 5G implementation?
(A) Its capital intensity makes rural integration a financial challenge.
(B) It decreases the speed of online transactions compared to 4G.
(C) It suffers from latency issues that prevent real-time fraud detection.
(D) It is fundamentally incompatible with blockchain and DLT applications.

**May/June 2009**

**58.** Which statement correctly identifies the function of HDFC Bank's EVA?
(A) It is an AI-powered chatbot that uses NLP to retrieve information.
(B) It is a robotic arm designed to count cash in branches.
(C) It is a biometric scanner used exclusively for employee attendance.
(D) It is a distributed ledger protocol used for cross-border settlements.

**Oct/Nov 2012**

**59.** Match the Zero Trust tenet principle (List I) with its core rationale (List II):
List I: (Tenet Principle)
P. Implicit trust zone elimination
Q. BYOD policy inclusion
R. Continual evaluation
S. Least Privilege Access
List II: (Rationale)
1. Assets act as if an attacker is present on the network.
2. Subject credentials alone are insufficient for device authentication.
3. Access given to any user is strictly on a 'need to know' basis.
4. Devices on the network may not be owned by the enterprise.
(A) P-4, Q-1, R-3, S-2
(B) P-2, Q-3, R-1, S-4
(C) P-1, Q-4, R-2, S-3
(D) P-3, Q-2, R-4, S-1

**May/June 2024**

**60.** Consider the following statements about Perimeter Security:
I It relies heavily on firewalls, perimeter routers, IPS, and WAF.
II Once an actor passes the perimeter, they are generally permitted to 'move laterally' across internal computers.
III It assumes that internal authentication is naturally stricter than external authentication.
IV Most successful cyber security incidents exploit this uninhibited lateral movement.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (III)
(B) (I), (II), and (IV)
(C) (II), (III), and (IV)
(D) (I), (III), and (IV)

**Oct/Nov 2022**

**61.** How does a Digital Banking Unit (DBU) assist a person who does not have connectivity or computing devices?
(A) By denying them service until they purchase a smartphone.
(B) By forcing them to travel to a brick-and-mortar branch city.
(C) By providing an 'assisted mode' where bank staff guide the user.
(D) By issuing them a physical checkbook to use exclusively.

**May/June 2007**

**62.** Which of the following is an exception and is NOT typically provided by a Digital Banking Unit (DBU)?
(A) Balance-check and Print passbook
(B) Loan applications and Transfer of funds
(C) Providing physical safe deposit locker boxes
(D) Tax payment and Bill payment

**Oct/Nov 2014**

**63.** Consider the following benefits of cloud adoption in Fintech:
I Self-service applications expansion
II Increased data management efficiency
III Agility to scale infrastructure relatively easily
IV Harnessing innovation potential for faster product-to-market times
V Eliminating the need for any form of data encryption

Downloaded from www.pdf.tube

Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (IV)
(B) (I), (III), (IV), and (V)
(C) (II), (III), (IV), and (V)
(D) (I), (II), (IV), and (V)

**May/June 2019**

**64.** Consider the following principles for CBDC Security Considerations:
I Security has to be the prime design concern since inception.
II Users with privileged roles should be subject to an enhanced risk management framework.
III The eco-system must ensure a single point of failure to centralize threat management.
IV CBDCs shall use cryptography that offers quantum resistance for futuristic scenarios.
V The entire eco-system should be vertically segregated into different segments.
Which of the above statement(s) is/are correct?
(A) (I), (II), (IV), and (V)
(B) (I), (III), (IV), and (V)
(C) (II), (III), (IV), and (V)
(D) (I), (II), (III), and (IV)

**Oct/Nov 2019**

**65.** Consider the following statements regarding the management of currency in India:
I The Reserve Bank of India derives necessary statutory powers from Section 22 of the RBI Act, 1934.
II Modern currency is a form of money issued exclusively by commercial banks without sovereign backing.
Which of the above statement(s) is/are correct?
(A) Only (I) is correct
(B) Only (II) is correct
(C) Both (I) and (II) are correct
(D) Neither (I) nor (II) is correct

**May/June 2020**

**66.** On what date did the RBI launch the first pilot for the retail digital Rupee (eRupee-R)?
(A) November 1, 2022
(B) December 1, 2022
(C) January 1, 2023
(D) April 1, 2022

**Oct/Nov 2009**

**67.** Modern Fintech is primarily driven by a combination of specific technologies. Which of the following statements correctly identifies these drivers?
I Artificial Intelligence (AI) provides insights into consumer behaviour.
II Big Data helps forecast market changes and develop new strategies.
III Blockchain enables decentralized transactions with heavy involvement of third-party intermediaries.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

**May/June 2013**

**68.** Which four properties differentiate variants of money?
(A) Value, Weight, Denomination, and Material
(B) Issuer, Form, Accessibility, and Technology
(C) Origin, Color, Interest rate, and Subsidies
(D) Taxation, Convertibility, Geography, and Language

**Oct/Nov 2020**

**69.** Which statement accurately summarizes the technology considerations required for deploying CBDC?
(A) The platform must be decentralized, scalable, and integrable.
(B) The platform should have routine planned downtimes to allow the economy to cool off.
(C) The platform must be strictly proprietary and prohibit cross-platform support to maximize security.
(D) The platform should run purely on non-encrypted public cloud servers to reduce costs.

**May/June 2016**

**70.** Which of the following is NOT listed as a key motivation for exploring the issuance of CBDC in India?
(A) Increasing operational costs for managing physical cash.
(B) Fostering financial inclusion.
(C) Bringing resilience, efficiency, and innovation in the payments system.
(D) Boosting innovation in the cross-border payments space.

NODIA

Oct/Nov 2007

**71.** Which of the following banks was NOT among the four banks identified for the first phase of the retail digital Rupee (eRupee-R) pilot?
(A) Punjab National Bank
(B) State Bank of India
(C) ICICI Bank
(D) YES Bank

May/June 2005

**72.** Which of the following is an incorrect statement regarding the best practices for Cloud Adoption in Fintech?
(A) Finance executives should discuss encryption policies and procedures to select technically feasible ones.
(B) Cloud services thrive on shared resources, therefore data segregation is heavily discouraged to save costs.
(C) Providers must be asked to demonstrate compliance certificates of the cloud service.
(D) A detailed disaster recovery plan should be obtained from reputable service providers.

Oct/Nov 2018

**73.** Which of the following statements concerning CBDC types is incorrect?
(A) Retail CBDC is meant primarily for retail transactions and is potentially available for use by all.
(B) Wholesale CBDC is intended for the settlement of interbank transfers and related wholesale transactions.
(C) Wholesale CBDC has the potential to transform the settlement systems for financial transactions.
(D) Retail CBDC is meant for restricted access to select institutions.

May/June 2017

**74.** Which combination of statements accurately reflects the primary functions of money?
I It acts as a medium of exchange for purchasing goods or services.
II It acts as a unit of account to express value in monetary terms.
III It acts as a store of value to be conserved for future purposes.
IV It acts strictly as an unexchangeable physical asset.
(A) (I), (II), and (III)
(B) (I), (II), and (IV)
(C) (II), (III), and (IV)
(D) (I), (III), and (IV)

Oct/Nov 2015

**75.** Under the principle of "Recoverability" in CBDC, what must happen if the system gets breached?
(A) The central bank must permanently shut down the digital currency network.
(B) Individual citizens must absorb all financial losses without any recourse.
(C) The breach should be covered up to prevent public panic.
(D) The system should recover quickly to minimize production impact.

May/June 2023

**76.** In the context of Fintech, how is cloud computing functionally characterized?
(A) A method of keeping all data locked in physical filing cabinets to prevent cyber theft.
(B) A system exclusively reserved for maintaining decentralized cryptocurrencies.
(C) A legacy on-premise technology that has grown increasingly difficult to upgrade.
(D) An agile infrastructure that lowers IT costs while remaining scalable.

Oct/Nov 2021

**77.** Consider the following statements regarding the offline capabilities of CBDC:
I The risk of "double-spending" exists in offline mode because the common ledger is not immediately updated.
II Wallets must be able to independently verify the authenticity of transactions without communicating with the server during the transaction.
III Offline transactions permanently eliminate the need for periodic network connectivity to synchronize local wallet balances.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

May/June 2011

**78.** Which of the following statements correctly highlights a key difference between a DBU and a traditional branch?

Click Here to Buy book on Amazon

(A) DBUs limit cash deposit and withdrawal services to standard banking hours.
(B) DBUs rely entirely on physical paper ledgers for end-to-end processing.
(C) DBUs prohibit the engagement of business correspondents.
(D) DBUs offer banking services, including cash deposit and withdrawal, 24x7.

**Oct/Nov 2006**

**79.** What is the most appropriate description of the Indirect (Two-Tier) model for CBDC issuance and management?
(A) The central bank is solely responsible for managing all aspects including account-keeping and transaction verification.
(B) The central bank issues CBDC through intermediaries to consumers.
(C) Intermediaries create and distribute their own private digital currencies completely independent of the central bank.
(D) The central bank issues physical notes directly to consumers without any banking intermediaries.

**May/June 2025**

**80.** In India, the Central Bank Digital Currency (CBDC) is formally referred to as:
(A) Cryptorupee (cRupee)
(B) BharatCoin (BRupee)
(C) E-Money (EM)
(D) Digital Rupee (eRupee)

**Oct/Nov 2013**

**81.** Which of the following statements correctly identifies the use case for the first pilot in the Digital Rupee - Wholesale segment (eRupee-W)?
(A) Facilitating cross-border personal remittances for retail customers.
(B) Issuing micro-loans to rural MSMEs.
(C) Settlement of secondary market transactions in government securities.
(D) Replacing physical ATM machines entirely across urban centers.

**May/June 2008**

**82.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): Digital Banking Units (DBUs) offer services exclusively in a self-service mode.
Reason (R): DBUs are designed to deliver digital banking products in an efficient, paperless environment.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2005**

**83.** Match the DBU mode/feature (List I) with its description (List II):
List I: (DBU Mode/Feature)
P. Self Service mode
Q. Assisted mode
R. End-to-end digital processing
S. Jan Samarth portal
List II: (Description)
1. Bank staff guide users for banking transactions.
2. Facilitates on-boarding to Government credit link schemes.
3. Applicable for small ticket retail and MSME loans.
4. Independent access to digital services by tech-savvy users.
(A) P-1, Q-4, R-2, S-3
(B) P-3, Q-2, R-1, S-4
(C) P-2, Q-3, R-4, S-1
(D) P-4, Q-1, R-3, S-2

**May/June 2010**

**84.** Which of the following is an incorrect statement regarding the key requirements for large-scale digital platforms running CBDC?
(A) They require zero downtime to keep the economy functioning.
(B) They mandate high volume and rate of transactions to avoid choking the platform.
(C) They must enforce centralization to restrict ecosystem participation.
(D) They require confidentiality, authentication, data integrity, and non-repudiation.

**May/June 2021**

**85.** Which of the following is an incorrect statement regarding the features of CBDC?
(A) CBDC is a sovereign currency issued by Central Banks in alignment with their

Downloaded from www.pdf.tube

Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (IV)
(B) (I), (II), IV, and (V)
(C) (II), (III), (IV), and (V)
(D) (I), (III), (IV), and (V)

**Oct/Nov 2024**

**43.** What is the cornerstone component in establishing a Zero Trust Architecture?
(A) Providing public Wi-Fi access in all bank branches.
(B) Micro-segmenting internal networks to arrest lateral movement.
(C) Removing Identity and Access Management systems.
(D) Granting maximum privilege access based on seniority.

**May/June 2006**

**44.** Consider the following statements regarding Axis Bank's digital automation:
I It has implemented AI across 125+ processes.
II It has deployed cognitive automation across 90 processes that required repetitive manual labour.
III Human prone error and objectivity remain entirely unaffected by RPA implementation.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

**Oct/Nov 2008**

**45.** Under the influence of 5G networks, what is the most appropriate vision for the future of bank customer service?
(A) Increased reliance on lengthy paper-based correspondences.
(B) Complete elimination of all customer support interfaces.
(C) High-resolution video streaming and AI-driven bot automation.
(D) Reverting exclusively to in-person branch appointments.

**May/June 2021**

**46.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): Chatbots and Robotic Process Automation (RPA) fulfill identical functions within a bank's digital transformation strategy.
Reason (R): Chatbots interface generally with the customer, whereas RPA generally interfaces with employees by automating repetitive IT tasks.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2010**

**47.** According to predictions, approximately how many 5G subscriptions will there be worldwide by 2025?
(A) 1 billion
(B) 2 billion
(C) 3 billion
(D) 5 billion

**May/June 2015**

**48.** What is the primary focus of chatbots currently utilized by leading commercial banks in India?
(A) Executing physical cash withdrawals
(B) Providing customer service through conversational apps
(C) Delivering localized weather forecasts
(D) Back-office data transcription

**Oct/Nov 2016**

**49.** Which of the following is NOT a vital component in establishing ZTA?
(A) Permanent authorization for recognized legacy devices.
(B) Proper network segmentation into smaller VLANs.
(C) Enhanced Identity and Access Management system.
(D) "Least Privilege Access" mode.

**May/June 2014**

**50.** Consider the following statements defining the Zero Trust Architecture (ZTA) concept:
I It no longer assumes that actors operating within the security perimeter should be automatically trusted.
II It must verify everything attempting to

NODIA

(D) Semi-structured

Oct/Nov 2012

**92.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): Embedded finance is perceived by some traditional financial institutions as a challenge to established banking methods.
Reason (R): Embedded finance allows non-financial enterprises to deliver banking-as-a-service (BaaS) products, embedding money within apps outside of traditional banking.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2019

**93.** What is the fundamental relationship between CBDC and current forms of money according to institutional visions?
(A) CBDC is aimed to completely replace the existing payment systems and physical cash.
(B) CBDC will be the sole currency accepted for government tax collections.
(C) CBDC is designed to complement current money as a payment avenue.
(D) CBDC is designed to inherently depreciate faster than physical cash to encourage spending.

Oct/Nov 2006

**94.** In a hypothetical economy, the central bank issues a digital currency. However, the retail consumers only interact with their respective commercial banks to open wallets, receive the currency, and lodge claims. The central bank only settles wholesale payments with the commercial banks.
Which CBDC issuance model does this represent?
(A) Direct model (Single Tier)
(B) Decentralized Cryptomodel
(C) Indirect model (Two-Tier)
(D) Offshore Ledger model

May/June 2007

**95.** A large commercial bank wishes to improve frontline customer interaction while simultaneously accelerating its back-office data entry tasks.
Which combination of technologies is best suited for this purpose?
(A) Private Blockchains for customer interaction and 5G networks for back-office.
(B) Chatbots for customers and Robotic Process Automation for back-office entry.
(C) Zero Trust Architecture for customer interaction and Open Banking APIs for data entry.
(D) Account aggregators for frontline interaction and Biometrics for back-office tasks.

Oct/Nov 2022

**96.** A central bank wants to introduce a digital currency specifically for the settlement of interbank transfers. This system will not be accessible to everyday retail consumers.
Which type of CBDC is the central bank implementing?
(A) CBDC-R (Retail)
(B) CBDC-W (Wholesale)
(C) Account-based CBDC for non-financial consumers
(D) Decentralized token protocol

May/June 2020

**97.** What is the most appropriate description of how transactions can be made using the retail digital Rupee (eRupee-R)?
(A) Transactions can only be executed via physical checks printed with QR codes.
(B) Transactions are strictly limited to Person to Person (P2P) transfers.
(C) Transactions automatically deduct a high transaction fee payable to the central bank.
(D) Transactions can be P2P or P2M via merchant QR codes.

Oct/Nov 2013

**98.** Which of the following is an incorrect statement regarding the rollout of 5G?
(A) 5G's primary disadvantage is its universal global coverage in all rural zones.
(B) By 2025, there will be about 3 billion 5G subscriptions worldwide.
(C) South Korea was the first country to adopt 5G on a large scale in April 2019.

Click Here to Buy book on Amazon

(D) 5G latency times are less than 1 millisecond.

**May/June 2005**

**99.** During the COVID-19 pandemic, a bank shifted to a WFH model, migrating workloads to nonenterprise cloud instances.
Which framework addresses this transition?
(A) Perimeter Firewalls
(B) Zero Trust Architecture (ZTA)
(C) Open Banking APIs
(D) Token-based CBDC

**Oct/Nov 2015**

**100.** Consider the following statements regarding Embedded Banking examples:
I Embedded payments enable users to make payments from a single location rather than digging for cash.
II Embedded lending eliminates the need for lengthy processes and costly paperwork at the point of purchase.
III Embedded insurance integration is decreasing due to consumer tech-savviness.
IV Embedded banking allows users to make investments, apply for loans, and manage transactions from one portal.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (III)
(B) (I), (II), and (IV)
(C) (II), (III), and (IV)
(D) (I), (III), and (IV)

**May/June 2025**

**101.** A fintech startup provides a payroll automation app. The startup wants to seamlessly connect its app to a traditional bank's backend operations to offer salary advances.
What technological mechanism will the bank primarily use to allow this secure third-party connection?
(A) Application Programming Interfaces (APIs)
(B) Cryptographic Hashes
(C) Near Field Communication (NFC)
(D) Zero Trust Orchestration

**Oct/Nov 2009**

**102.** Which statement accurately differentiates cognitive automation from cognitive engagement?
(A) Automation applies ML for expertise, while engagement personalizes interaction.
(B) Cognitive automation focuses on unlocking unstructured data for personalized customer offerings, while cognitive engagement uses RPA for repetitive tasks.
(C) Both cognitive automation and cognitive engagement are identical processes exclusively used for hardware maintenance.
(D) Cognitive automation is purely an offline process, whereas cognitive engagement relies entirely on public blockchains.

NODIA

**May/June 2017**

**103.** Match the emerging technology (List I) with its core operational advantage (List II):
List I: (Emerging Technology)
P. API
Q. Big Data Analytics
R. Machine Learning
S. Zero Trust Architecture
List II: (Operational Advantage)
1. Employs micro-segmentation and assumes no implicit trust within the network.
2. Acts as a structured method for one software to provide services to another.
3. Provides predictive insights by translating incredible volumes of unstructured data.
4. Uses statistical techniques to give computers the ability to learn without explicit programming.
(A) P-1, Q-2, R-3, S-4
(B) P-2, Q-3, R-4, S-1
(C) P-3, Q-4, R-1, S-2
(D) P-4, Q-1, R-2, S-3

**Oct/Nov 2024**

**104.** How does Robotic Process Automation practically achieve "zero infrastructure cost" when implemented in a bank?
(A) It requires the complete replacement of all desktop computers with thin clients.
(B) It eliminates all internet bandwidth usage.
(C) It is an open-source software that banks are legally barred from paying for.
(D) It uses UI automation to interact with existing legacy software interfaces.

**May/June 2016**

**105.** Match the specific business application (List I) with its corresponding Fintech area (List II):
List I: (Business Application)
P. Rapid, automated credit issuance to retail clients
Q. Faster checkout processes via mobile

applications
R. Decentralized, immutable transaction ledger
S. Robo-advisory for mutual funds and stocks

List II: (Fintech Area)
1. Blockchain
2. Digital wealth management
3. Digital lending
4. Payments

(A) P-4, Q-3, R-2, S-1
(B) P-1, Q-2, R-3, S-4
(C) P-3, Q-4, R-1, S-2
(D) P-2, Q-1, R-4, S-3

**Oct/Nov 2011**

**106.** Match the specific CBDC term/feature (List I) with its contextual meaning (List II):

List I: (CBDC Term/Feature)
P. eRupee-W
Q. eRupee-R
R. CUG
S. Double-spending

List II: (Meaning)
1. Utilizing a digital token more than once without ledger synchronization.
2. Closed User Group participating in the pilot project.
3. Digital token aimed at the Wholesale segment for inter-bank efficiency.
4. Digital token meant for the retail segment, distributed through intermediaries.

(A) P-4, Q-3, R-1, S-2
(B) P-3, Q-4, R-2, S-1
(C) P-2, Q-1, R-4, S-3
(D) P-1, Q-2, R-3, S-4

**May/June 2022**

**107.** A bank evaluating a public blockchain like Bitcoin realizes it can only process seven transactions per second, compared to Visa's 24,000.
This specific operational limitation is referred to as:
(A) Scalability issue
(B) Privacy restriction
(C) Storage barrier
(D) Regulatory impediment

**Oct/Nov 2023**

**108.** What is the most appropriate role of "smart contracts" in the context of 5G and fraud detection?
(A) To foster trust and promote automated agreements via blockchain support.
(B) To manually verify physical signatures on loan documents.
(C) To restrict network bandwidth for suspicious devices.
(D) To legally bind customers to exclusive mobile banking contracts.

**May/June 2010**

**109.** A bank's security team notices fraudulent transactions happening in real-time.
Which specific AI application allows the bank to identify this fraudulent behaviour as it occurs and predict the next pattern of suspicious behaviour?
(A) Robotic Process Automation
(B) Cognitive Insight
(C) API account aggregation
(D) Artificial Intelligence Fraud detection systems

**Oct/Nov 2010**

**110.** Which statement accurately distinguishes a Consortium Blockchain from a Private Blockchain?
(A) A Consortium Blockchain is governed by a single organization, while a Private Blockchain is completely decentralized and open to the public.
(B) A Consortium Blockchain uses zero encryption, whereas a Private Blockchain uses post-quantum encryption.
(C) A Consortium Blockchain shares responsibility, while a Private Blockchain is single-governed.
(D) A Consortium Blockchain restricts transaction speed to 7 per second, unlike a Private Blockchain.

**May/June 2008**

**111.** A bank's compliance department is overwhelmed with unstructured data formats such as emails, videos, and social media posts that must be analyzed without pre-tagging.
Which specific AI technology is explicitly tailored to handle and extract data insights from these unstructured datasets?
(A) Traditional relational databases
(B) Smart Contracts
(C) Legacy 4G networks
(D) Cognitive Analytics

Downloaded from www.pdf.tube

**33.** (C) 10-15 minutes
The implementation of robotic process automation has significantly transformed the efficiency of loan processing in the banking sector. By automating data entry, verification, and documentation tasks, banks have managed to reduce processing times drastically. Modern RPA solutions can now complete complex loan processing workflows in as little as ten to fifteen minutes, a major improvement over traditional manual methods.

**34.** (D) By using portable mobile banks to deliver VR experiences.
The rollout of 5G technology enables banks to deploy mobile pop-up branches that provide advanced services in remote or temporary locations. These portable units leverage the high bandwidth and low latency of 5G to deliver immersive experiences such as virtual reality banking. This allows customers to interact with expert advisors or explore financial products in high-definition without needing a traditional brick-and-mortar branch.

**35.** (B) Only (II) is correct
ICICI Bank has successfully integrated software robotics into its operations to emulate human actions across various business processes. This digital transformation has led to significant improvements in productivity by increasing accuracy to one hundred percent. While the technology has enhanced response times for customers, the primary benefit highlighted by the bank is the elimination of manual errors and the resulting operational excellence.

**36.** (C) Big Data Analytics - 91%
Reports from September 2020 regarding technology adoption in the global financial services industry projected a high implementation rate for several innovations. Among these, big data analytics stood out with a predicted adoption rate of ninety-one percent. This high percentage reflects the industry's focus on leveraging data to improve risk management, customer insights, and operational efficiency across the worldwide banking landscape.

**37.** (A) (I), (II), and (III)
Robotic process automation is designed to handle mundane, repetitive, and rule-based tasks across various banking software platforms. By operating at the individual data field level, RPA systems can seamlessly move information between applications without human intervention. This implementation allows professional staff to move away from clerical duties and focus more on high-value work, such as client advisory and complex problem-solving.

NODIA

**38.** (C) Assertion (A) is true, but Reason (R) is false.
Zero trust architecture is a highly effective security framework that mitigates cyber incidents by preventing uninhibited lateral movement within a network. Unlike perimeter-based security, zero trust does not assume that internal actors are safe. Instead, it continuously authenticates and authorizes every access request and monitors internal network activity, ensuring that security protocols are applied consistently to all users and devices.

**39.** (A) (I), (II), and (III)
G is indeed the fifth generation of cellular networks and is based on OFDM technology. It offers ultra-low latency, often close to or below 1 millisecond, and significantly higher speeds compared to 4G, ranging from ten to one hundred times faster. However, it does not operate exclusively on sub-2 GHz bands, as it also uses higher frequency bands like millimeter waves.

**40.** (D) "Code For Bank"
To advance its artificial intelligence mission, the State Bank of India launched a national hackathon aimed at collaborating with developers and startups. This initiative, titled "Code For Bank," focused on identifying innovative solutions in areas such as predictive analytics, fintech, and automated bots. Such events allow major financial institutions to tap into external expertise and accelerate their digital transformation through creative technological applications.

**41.** (B) Digital wealth management - Manual paper-based ledger storage
Modern fintech is divided into several core areas, including digital lending for quick credit and payments for streamlining transactions. Blockchain technology is utilized for housing encrypted and decentralized transactions. In contrast, digital wealth management focuses

prevent editing.

V Successive blocks reinforce the prior block's verification, making the chain tamper-evident.

(A) (I), (II), (III), and (V)
(B) (II), (III), IV, and (V)
(C) (I), (II), (IV), and (V)
(D) (I), (II), (III), (IV), and (V)

**May/June 2006**

**119.** A bank receives KYC documents daily. To reduce TAT, the bank uses OCR to read data and match it with forms.
Which technology is best suited for this?
(A) Robotic Process Automation (RPA)
(B) 5G streaming
(C) Embedded Lending
(D) Public Blockchain

**Oct/Nov 2017**

**120.** A customer named Rohan maintains a savings account with Bank X, a loan with Bank Y, and an investment portfolio with Bank Z.
Which Open Banking feature will allow Rohan to manage all these financial relationships from a single mobile application?
(A) Account aggregation
(B) Better borrowing terms
(C) Better payment options
(D) Embedded insurance

**May/June 2009**

**121.** A financial institution is migrating to a public cloud to gain economies of scale but is concerned about data security on shared resources. To mitigate this risk, the institution requires a combination of shared resource benefits with increased security.
Which best practice of cloud adoption addresses this specific need?
(A) Abandoning all compliance checks
(B) Moving exclusively to physical ledgers
(C) Refusing to adopt disaster recovery plans
(D) Data segregation and data management

**Oct/Nov 2007**

**122.** A bank's marketing team utilizes Big Data to understand each unique customer and design specific credit card offers suited to individual spending habits.
Which major benefit of Big Data Analytics does this scenario primarily illustrate?
(A) Superior Risk Assessment
(B) Enhanced Fraud Detection
(C) Product Personalization
(D) Workplace Improvements

**May/June 2015**

**123.** An intermediary verifies the identity of an individual attempting to utilize a Central Bank Digital Currency. Based on this identity verification process,
which form of CBDC is being used?
(A) Token-based CBDC
(B) Bearer-instrument CBDC
(C) Account-based CBDC
(D) Unregulated cryptocurrency

**Oct/Nov 2020**

**124.** A retail bank plans to upgrade its physical branch by introducing instant facial recognition and AR/VR banking capabilities to enhance customer experience.
Which next-generation network technology is essential to provide the required low latency and high bandwidth for these applications?
(A) 5G Network
(B) Optical Character Recognition (OCR)
(C) Robotic Process Automation (RPA)
(D) Consortium Blockchain

**May/June 2011**

**125.** An elderly customer from a rural area visits a Digital Banking Unit (DBU) but does not possess a smartphone or digital literacy.
How will the DBU ensure this customer can still perform banking transactions?
(A) By redirecting the customer to a traditional branch.
(B) By offering services in 'Assisted mode' with staff guidance.
(C) By issuing a physical ATM card and leaving the customer to figure it out.
(D) By denying service as DBUs strictly serve only self-service tech-savvy individuals.

www.nodia.in

Click Here to Buy book on Amazon

with traditional banking interfaces, making financial management a background process for consumers.

**17.** (A) The engineering of intelligent machines and computer programs.
Within the field of computer science, artificial intelligence is formally defined as the engineering of intelligent machines and computer programs. It focuses on creating systems capable of performing tasks that typically require human intelligence, such as visual perception, speech recognition, and decision-making. AI involves developing algorithms that allow computers to learn from data, reason through problems, and improve over time.

**18.** (A) P-2, Q-4, R-1, S-3
Embedded finance integrates financial services directly into non-financial platforms to streamline user experiences. Embedded payments and card systems facilitate faster checkouts and electronic fund transfers through virtual mediums. Additionally, embedded lending allows point-of-purchase loan applications, while embedded investments offer centralized platforms for market trading. These models eliminate friction by providing financial tools within the context of the customer journey.

**19.** (D) It increases human error by requiring complex manual record-keeping processes.
Blockchain technology offers numerous benefits to the banking sector, including accelerated international transfers and reduced operational costs through automation. By creating a visible and redundant audit trail, it significantly enhances fraud prevention and transparency. Because it automates record-keeping and utilizes cryptographic verification, the technology is designed to reduce rather than increase human error in complex financial processing tasks.

**20.** (A) It streamlines compliance verification, auditing, and reporting processes.
Big data analysis provides banks with a significant strategic advantage in meeting their regulatory obligations. By processing massive datasets, these tools can automate and streamline compliance verification, internal auditing, and official reporting processes. This efficiency helps financial institutions remain compliant with evolving laws, reduces the risk of human oversight, and ensures that reporting is both accurate and delivered on time.

**21.** (A) Only (I) is correct
Machine learning is a specialized branch of artificial intelligence where algorithms are designed to learn from data and generate foresights without being explicitly programmed for every scenario. It is particularly effective for complex tasks where designing traditional rule-based algorithms is difficult. By identifying patterns within large datasets, these systems can improve their performance and accuracy independently over time through experience.

**22.** (B) Electromagnetic Telegraphy
The banking and financial sector is currently being transformed by several core emerging technologies, including blockchain, robotic process automation, and zero trust security models. These innovations focus on increasing efficiency, transparency, and data protection. Conversely, electromagnetic telegraphy is a legacy communication technology from the past and does not play a role in the modern digital transformation of financial services.

**23.** (D) By offering a platform for investing without leaving the current site.
Embedded investments streamline the user experience by integrating brokerage and trading capabilities directly into non-financial applications. This allows users to invest in stocks or mutual funds without having to leave their current platform or visit a separate physical brokerage firm. By removing the need for multiple app transitions, this model simplifies the investment process and encourages more frequent user engagement.

**24.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Blockchain technology eliminates the risk of data tampering by creating a trusted and irreversible record of transactions. This security is achieved because each new block added to the chain reinforces the verification of all prior blocks. This sequential linking makes any attempt to alter past data immediately evident and extremely difficult,

NODIA

these applications improve risk assessment and customer retention strategies by leveraging vast amounts of historical data.

**9.** (B) Consortium Blockchain - Governed exclusively by a single organization
Blockchain technology is categorized into various types based on governance and access. While public blockchains like Bitcoin are open to everyone, private blockchains are restricted to specific authorized users. Consortium blockchains differ from private ones because they are governed by a group of organizations rather than a single entity, ensuring shared responsibility and collaborative decision-making within the network.

**10.** (C) Account aggregation - Consolidating all accounts into one view.
Open banking facilitates the sharing of financial data between banks and third-party providers with consumer consent. A primary benefit of this system is account aggregation, which allows customers to view and manage all their various financial accounts within a single digital interface. This consolidation simplifies financial tracking, enhances transparency, and enables more informed decision-making regarding personal or business finances.

**11.** (A) (I) and (II) only
Artificial intelligence is a broad field of computer science where machine learning serves as a fundamental building block. Cognitive computing expands on these concepts by integrating disciplines such as natural language processing, computer vision, and human-computer interaction to simulate human thought processes. These technologies are deeply interconnected, with AI systems often relying on machine learning algorithms to achieve intelligent outcomes.

**12.** (C) Central banks act as the exclusive data aggregators and intermediaries for all open banking transactions.
Open banking involves multiple participants including customers, financial service providers, and innovative enterprises. While it allows for product innovation and more efficient financial instruments, the role of central banks is primarily regulatory rather than acting as exclusive data aggregators. Data sharing is usually facilitated through secure application programming interfaces between authorized financial institutions and third-party service providers.

**13.** (A) It links blocks via cryptographic hashes of previous data to ensure immutability.
Blockchain technology ensures data integrity by linking individual blocks through cryptographic hashes of preceding data. This structure creates an irreversible and tamper-evident chain where any modification to a single block would be immediately detected across the network. The decentralized nature of the ledger, combined with this sequential cryptographic verification, establishes a highly secure and trusted record of transactions.

**14.** (C) It standardizes product offerings so that all unique customers receive the exact same generic services.
Big data analytics provides significant advantages to the banking sector by enabling individual-level transaction tracking and risk identification. It also assists in managing customer feedback effectively and in a timely manner. However, its primary value lies in personalization rather than standardization, as it allows banks to move away from generic services toward tailored offerings based on unique customer profiles.

NODIA

**15.** (D) It allows for the processing of large, unstructured datasets without pre-tagging.
Cognitive analytics represents an advanced form of data processing that mimics human reasoning. Unlike traditional methods that often require structured data or extensive manual tagging, cognitive systems can analyze vast amounts of unstructured information without prior categorization. This capability allows financial institutions to extract valuable insights from complex sources like documents, emails, and social media with greater efficiency and accuracy.

**16.** (A) Invisible banking
The convergence of advanced technologies such as artificial intelligence, internet of things, and banking as a service aims to create an experience known as invisible banking. In this model, financial transactions and services are seamlessly integrated into everyday activities and platforms. This eliminates the need for manual interactions

# ANSWERS

1. (D) To bridge bank backend operations and third-party frontend experiences.
API banking platforms serve as a crucial technological bridge within the modern financial ecosystem. They allow financial institutions to securely expose their backend data and services to third-party developers and fintech firms. This connectivity enables the creation of innovative frontend experiences for customers while maintaining the robust security and processing power of traditional banking infrastructure.

2. (D) (I), (II), and (III)
Public blockchains operate as open networks requiring significant computing power and providing transparent transaction histories. Private blockchains remain decentralized but are strictly controlled by a single entity regarding participant authorization. Consortium blockchains involve multiple organizations sharing responsibility for maintenance and governance. Together, these categories offer diverse solutions for various commercial needs including privacy and shared accountability.

3. (C) They offer digital banking services without requiring physical branches.
Neo-banks represent a modern shift in the financial industry by offering comprehensive banking services through purely digital platforms. Unlike traditional banks, these institutions do not maintain physical brick-and-mortar branch locations. This operational model significantly reduces overhead costs, allowing for more competitive rates and streamlined customer experiences delivered entirely through mobile apps and web-based interfaces.

4. (C) Analyzing digital marketing data to observe changes in consumer behavior.
Predictive analytics in the commercial sector involves using historical data and statistical algorithms to identify future trends. By analyzing digital marketing data, businesses can observe subtle changes in consumer behavior and preferences. This allows organizations to anticipate market shifts, tailor their product offerings, and optimize marketing strategies to enhance customer engagement and drive better financial outcomes.

5. (B) Data containing keywords that can be used for identification and processing.
Semi-structured data represents a category of information that does not reside in a traditional relational database but contains organizational properties. It includes elements like keywords, tags, or metadata that facilitate easier identification and processing. Common examples include XML or JSON files, where the data format is flexible yet contains enough structure for analytical tools to parse effectively.

6. (B) P-3, Q-4, R-1, S-2
Artificial intelligence enhances banking through diverse applications such as real-time fraud detection using location data and automated compliance monitoring. It further streamlines operations by utilizing virtual assistants for frontline services and generating deep insights from behavior patterns. These technological integrations allow banks to lower operational costs while significantly improving the speed and quality of customer experiences.

7. (C) 28%
The annual report of the Reserve Bank of India for 2020-21 highlighted a significant surge in digital payment adoption. According to the data, total digital transaction volumes grew by twenty-eight percent compared to the previous year. This growth underscores the increasing preference for electronic payment methods among consumers and businesses, driven by improved digital infrastructure and shifting transaction habits.

8. (B) P-4, Q-2, R-1, S-3
Big data analytics enables banks to track individual transactional activities for enhanced security and identify risky profiles through predictive capabilities. These tools also help in building detailed client profiles to foster long-lasting interactions and create personalized products based on specific needs. Collectively,

Downloaded from www.pdf.tube

thereby establishing a robust and tamper-evident digital ledger.

**25.** (A) Only (I) is correct
In blockchain technology, the timestamp serves as a critical validation tool that confirms transaction data existed at the specific time the block was released. Once a block is added to the chain, it cannot be easily edited or moved. This permanent and sequential structure ensures that the transaction history remains chronological and resistant to unauthorized modifications or historical record deletions.

**26.** (D) A system for sharing data with user consent to provide financial services.
Open banking is a financial services framework that allows for the secure sharing of customer data between banks and third-party providers, strictly based on user consent. This system utilizes application programming interfaces to facilitate data exchange, enabling the development of personalized financial products and services. The primary goal is to enhance competition, foster innovation, and provide customers with more financial flexibility.

**27.** (D) (II), (I), (III)
The progression of artificial intelligence applications in the finance industry typically begins with foundational cognitive automation for repetitive tasks. This is followed by cognitive insight, which involves extracting deep meaning and patterns from large datasets for better decision-making. Finally, cognitive engagement represents the most complex stage, where AI systems interact directly with customers to provide personalized and proactive financial services.

**28.** (A) The use of financial instruments or services by a non-financial supplier.
Embedded banking refers to the integration of financial instruments and services directly into the platforms of non-financial companies. This allows businesses such as retail brands or service providers to offer payments, lending, or insurance within their own ecosystem. By placing banking services where consumers already interact, companies can provide a more seamless and convenient experience without requiring customers to visit a bank.

**29.** (C) The ease of reversing transactions without the consent of network nodes.
Blockchain technology faces several inherent challenges, including scalability constraints due to limited transaction processing speeds and storage issues as the ledger grows. Additionally, privacy can be a concern on public networks where data is accessible to all nodes. However, the ease of reversing transactions is not a limitation, as blockchains are designed specifically to ensure transaction immutability and permanence.

**30.** (D) Deleting legacy customer data to free up server storage.
When banks create a 360-degree image of their consumers, they combine personal and transactional data to gain comprehensive insights. This allows them to track spending habits, segment customers into specific profiles, and customize product offerings to meet individual needs. Deleting legacy customer data is not a typical outcome of this process, as historical data is valuable for long-term trend analysis.

**31.** (C) Conducting emotional intelligence assessments of bank employees
Robotic process automation is highly effective for streamlining repetitive and rule-based tasks such as opening bank accounts, processing mortgage loans, and conducting anti-money laundering checks. These processes rely on structured data and clear logic. However, RPA cannot automate tasks requiring human judgment or empathy, such as conducting emotional intelligence assessments of employees, which remain a uniquely human responsibility.

**32.** (B) Devices on the network must be owned and configurable exclusively by the enterprise.
Zero Trust Architecture operates on the principle that no resource is inherently trusted, regardless of its location on the network. It requires continuous evaluation of every asset's security posture and applies consistent policies across enterprise and non-enterprise infrastructure. Importantly, the framework recognizes that not all devices on the network are owned by the enterprise, necessitating secure management of third-party and personal equipment.

NODIA

Oct/Nov 2021

**112.** Which of the following is an incorrect statement regarding the anticipated impact of 5G on physical wallets?
(A) 5G's high-speed transaction capabilities will accelerate the adoption of digital payments.
(B) Physical wallets will become entirely obsolete instantly upon the launch of 5G.
(C) A large percentage of senior millennials have completely transitioned to mobile payments.
(D) Additional wearables and IoT devices will make digital wallets across channels more attractive.

May/June 2023

**113.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): RPA greatly simplifies the customer on-boarding procedure in banks.
Reason (R): RPA uses optical character recognition (OCR) to gather data from KYC documents and automates client management interface entry.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Oct/Nov 2019

**114.** A telecom company aims to bring much-needed financial inclusion to remote populations by enabling real-time translation and flawless VR mobile banking.
Which technology serves as the foundational enabler for this scenario?
(A) Legacy 3G networks
(B) 5G Network
(C) Private Data Centers
(D) Physical brick-and-mortar expansion

May/June 2013

**115.** Which of the following is an exception to the benefits a Fintech firm expects when adopting Cloud Computing?
(A) Increased flexibility and scalability
(B) Better security-driven innovation
(C) Harnessing innovation potential for agile market adaptation
(D) Mandatory reliance on legacy hardware for all infrastructure maintenance

Oct/Nov 2016

**116.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option.
Assertion (A): The use of offline transactions in CBDC brings a technical risk of double-spending.
Reason (R): Offline transactions operate without instantly updating the common ledger of the CBDC server.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2018

**117.** Arrange the following steps in the correct chronological order of how a Blockchain functions during an asset transfer:
I The transaction is logged as a "block" of data.
II The blocks validate the exact timing and sequence of transactions.
III The block is securely linked to the ones that come before and after it.
IV The successive block reinforces the prior block's verification, providing immutability.
(A) (I), (II), (III), (IV)
(B) (I), (III), (II), (IV)
(C) (II), (I), (III), (IV)
(D) (I), (II), (IV), (III)

Oct/Nov 2008

**118.** Consider the sequential mechanics of Blockchain:
I A transaction is logged as a "block" of data.
II The data block can store information like who, what, when, and how much.
III The block validates the exact timing and sequence of transactions.
IV The blocks are linked securely together to

Click Here to Buy book on Amazon

on using technology to automate investment processes and portfolio management, moving away from legacy manual paper-based record-keeping toward sophisticated digital platforms.

**42.** (B) (I), (II), (IV), and (V)
Robotic process automation is applied in banking to automate suspicious activity reporting, customer onboarding via KYC document processing, and mortgage lending workflows. It also eliminates transcription errors in account opening by automating data entry. While RPA is excellent for these rule-based tasks, it is generally not used for providing high-level advisory on complex personal wealth management, which requires human judgment.

**43.** (B) Micro-segmenting internal networks to arrest lateral movement.
A cornerstone of establishing a zero trust architecture is the implementation of micro-segmentation within internal networks. This process involves dividing the network into smaller, isolated zones to arrest lateral movement by potential attackers. By restricting access between these segments and requiring verification for every connection attempt, organizations can significantly limit the impact of a security breach and better protect sensitive financial data.

**44.** (A) (I) and (II) only
Axis Bank has made significant strides in digital transformation by implementing artificial intelligence across more than one hundred and twenty-five different business processes. Additionally, the bank has deployed cognitive automation to handle ninety processes that previously required repetitive manual labor. These initiatives are designed to improve operational efficiency and reduce the human errors that often occur during manual data handling and processing.

**45.** (C) High-resolution video streaming and AI-driven bot automation.
The integration of 5G technology is expected to redefine the future of bank customer service by enabling high-resolution video streaming and advanced AI-driven bot interactions. These capabilities allow for more immersive and responsive support experiences that can be delivered in real-time. Customers will benefit from faster resolution of issues and more personalized guidance, reducing the need for physical branch visits or lengthy correspondence.

**46.** (D) Assertion (A) is false, but Reason (R) is true.
Chatbots and robotic process automation serve distinct roles within a bank's digital strategy. While both involve automation, chatbots are primarily designed as customer-facing interfaces for conversational interaction. In contrast, RPA is typically used for backend operations to automate repetitive tasks for employees. Therefore, they do not fulfill identical functions but rather complement each other by addressing different aspects of the banking experience.

**47.** (C) 3 billion
The global adoption of 5G technology is projected to grow rapidly over the coming years. Market predictions suggest that by 2025, there will be approximately three billion 5G subscriptions worldwide. This widespread availability of high-speed, low-latency connectivity will provide the necessary foundation for advanced financial services, including ubiquitous mobile banking, real-time fraud detection, and the expansion of the internet of things.

**48.** (B) Providing customer service through conversational apps
Major commercial banks in India have deployed chatbots primarily to enhance customer service through conversational applications. These AI-powered tools are designed to handle frequently asked questions, provide account information, and assist with basic transactions on a twenty-four-seven basis. By providing instant responses through familiar messaging interfaces, chatbots improve customer accessibility and reduce the workload on traditional human-led call centers.

**49.** (A) Permanent authorization for recognized legacy devices.
Establishing a zero trust architecture requires several vital components, including enhanced identity and access management and the implementation of a least privilege access model. Proper network segmentation into smaller VLANs is also essential for security. However, granting permanent authorization for recognized legacy devices contradicts the core principle of

NODIA

often lack the same level of access as urban centers due to the high cost of infrastructure deployment, contrary to any claims of immediate global coverage.

**99.** (B) Zero Trust Architecture (ZTA)
When a bank shifts to a work-from-home model and migrates workloads to non-enterprise cloud instances, zero trust architecture is the most appropriate framework to address the transition. ZTA ensures that every access request is verified regardless of where the employee is located or which network they are using. This approach provides consistent security for sensitive financial data, even when it is accessed from outside traditional perimeters.

**100.** (B) (I), (II), and (IV)
Embedded banking examples include payments that allow for faster checkouts from a single location and lending services that provide point-of-purchase financing without complex paperwork. These models enable users to manage various financial tasks, such as investing and loan applications, directly within a single digital portal. Contrary to trends, embedded insurance integration is actually increasing as consumer platforms look to provide more comprehensive services to their users.

**101.** (A) Application Programming Interfaces (APIs)
To allow a third-party fintech startup to connect securely to its backend operations, a bank will primarily use application programming interfaces. APIs serve as a standardized and secure technological bridge that facilitates data exchange and service integration between different software systems. This connectivity enables the development of innovative financial products, like salary advance apps, while ensuring that the bank maintains control over its core infrastructure.

**102.** (A) Automation applies ML for expertise, while engagement personalizes interaction.
Cognitive automation involves using machine learning and artificial intelligence to automate complex tasks that require a level of expertise or insight beyond simple rule-based processing. On the other hand, cognitive engagement focuses on using these technologies to personalize customer interactions and provide proactive, human-like support. While both use AI, their primary goals differ between improving operational expertise and enhancing the quality of direct customer relationships.

**103.** (B) P-2, Q-3, R-4, S-1
Emerging technologies provide diverse advantages, such as APIs offering structured methods for software communication and big data analytics delivering predictive insights from unstructured information. Machine learning uses statistical techniques to enable computers to learn from data independently. Finally, zero trust architecture improves security by employing micro-segmentation and assuming no implicit trust within the network, protecting sensitive financial assets from both internal and external threats.

**104.** (D) It uses UI automation to interact with existing legacy software interfaces.
Robotic process automation practically achieves near-zero infrastructure costs by using user interface automation to interact with a bank's existing legacy software. This means the software robots can perform tasks across the current digital landscape without requiring expensive changes to the underlying IT systems. By leveraging the existing technology stack, banks can quickly implement automation and gain operational efficiencies with very little additional hardware investment.

**105.** (C) P-3, Q-4, R-1, S-2
Different fintech areas address specific business needs, such as digital lending for rapid credit issuance and payments for streamlining mobile checkout processes. Blockchain technology provides a decentralized and immutable ledger for secure transactions, while digital wealth management utilizes robo-advisory tools to manage investments in stocks and mutual funds. These diverse applications together form a comprehensive ecosystem that modernizes various aspects of traditional financial services and retail banking.

**106.** (B) P-3, Q-4, R-2, S-1
Central bank digital currency pilots use specific terms like eRupee-W for wholesale interbank efficiency and eRupee-R for retail tokens distributed through intermediaries. A closed user

Downloaded from www.pdf.tube

remote areas continue to rely on older, slower network generations.

**58.** (A) It is an AI-powered chatbot that uses NLP to retrieve information.
HDFC Bank's Electronic Virtual Assistant, known as EVA, is an artificial intelligence-powered chatbot designed to enhance customer service. It utilizes natural language processing to understand user queries and retrieve relevant information from the bank's database instantly. By providing a conversational interface for answering frequently asked questions, EVA offers a fast and efficient way for customers to interact with the bank at any time.

**59.** (C) P-1, Q-4, R-2, S-3
Zero trust principles include the elimination of implicit trust zones, assuming an attacker is always present on the network. The framework also incorporates personal devices through BYOD policies and requires continual evaluation of device and user credentials. Finally, the least privilege access principle ensures that users are only given the specific permissions necessary for their roles, minimizing potential damage from any security breach.

**60.** (B) (I), (II), and (IV)
Traditional perimeter security relies heavily on firewalls and routers to protect the network boundary. However, once an actor passes this perimeter, they are often permitted to move laterally across internal systems with minimal restriction. Most successful cyber security incidents exploit this lack of internal monitoring. Zero trust architecture addresses these weaknesses by requiring continuous verification for all activities, regardless of their network location.

**61.** (C) By providing an 'assisted mode' where bank staff guide the user.
Digital banking units are designed to be inclusive by offering an assisted mode for individuals who may lack connectivity or personal computing devices. In this mode, bank staff are available to guide users through their digital transactions and help them navigate the platform. This ensures that the benefits of digital banking are accessible to all segments of the population, including those with limited digital literacy.

NODIA

**62.** (A) Increasing operational costs for managing physical cash.
The exploration of a central bank digital currency in India is driven by several key motivations, including fostering financial inclusion and improving the efficiency of the payments system. CBDC also aims to bring resilience and innovation to cross-border transactions. Reducing the high operational costs associated with managing physical cash is a primary goal, rather than increasing them, making digital currency an attractive alternative for the central bank.

**63.** (A) (I), (II), and (III), and (IV)
Cloud adoption in the fintech sector offers numerous benefits, such as the ability to scale infrastructure easily and improve data management efficiency. It also enables the rapid development of self-service applications and helps businesses bring innovative products to market faster. While the cloud enhances many operations, it does not eliminate the need for data encryption, which remains a critical component of financial security.

**64.** (A) (I), (II), (IV), and (V)
The security of a central bank digital currency system must be a prime design concern from inception, incorporating features like quantum-resistant cryptography. Privileged users within the ecosystem should be subject to enhanced risk management frameworks to prevent abuse. Additionally, the system should be vertically segregated to improve resilience and avoid single points of failure, ensuring that the digital currency remains secure and reliable.

**65.** (A) Only (I) is correct
In India, the Reserve Bank of India holds the statutory power to manage the issuance and regulation of currency under Section twenty-two of the RBI Act of 1934. Modern currency is a sovereign form of money backed by the government, rather than being issued exclusively by private commercial banks. This legal framework ensures the stability and public trust necessary for a functional national monetary system.

continuous verification, which requires that all devices be re-evaluated regularly.

**50.** (A) (I), (II), and (IV)
Zero trust architecture is defined by the principle of never assuming trust for any actor, even those within the traditional security perimeter. It requires rigorous verification of every connection attempt before granting access to systems. Additionally, the framework encourages the micro-segmentation of internal networks into smaller zones to prevent unauthorized lateral movement, ensuring a more resilient and secure environment for financial data.

**51.** (A) Only (I) is correct
Fintech is broadly defined as technology-enabled innovation in financial services that can result in new business models, applications, processes, or products. These innovations have a material effect on how financial services are provided and consumed. The field encompasses a wide range of technologies, including mobile banking, blockchain, and artificial intelligence, all aimed at making financial transactions more efficient and accessible.

**52.** (D) By using UI automation to work within existing legacy systems.
Robotic process automation achieves a near-zero infrastructure cost in financial services by utilizing user interface automation. This allows software robots to interact with existing legacy systems just as a human operator would, without requiring significant changes to the underlying IT architecture. By working within the current software environment, banks can automate complex workflows quickly and cost-effectively, avoiding expensive system replacements.

**53.** (C) P-4, Q-3, R-1, S-2
Indian banks have pioneered various AI initiatives, such as SBI's national hackathon and HDFC's Electronic Virtual Assistant for customer service. ICICI Bank has focused on deploying software robotics across hundreds of business processes to emulate human actions, while Axis Bank launched an AI-enabled app for conversational banking. These diverse technological efforts demonstrate the industry's commitment to improving efficiency and enhancing the overall customer experience.

**54.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
The deployment of 5G technology will significantly expand the opportunities for the internet of things within the banking sector. This growth is driven by 5G's ability to offer much lower latency and improved connectivity, which allows a vast number of smart devices to interact in real-time. These interconnected gadgets can provide more data points for banks, leading to personalized services and enhanced operational monitoring.

**55.** (A) As an environment where an attacker is assumed to be constantly present.
Within the context of zero trust architecture, the enterprise private network must be perceived as an environment where an attacker is assumed to be constantly present. This shift in mindset necessitates the implementation of strict security controls and continuous monitoring for all internal activities. By treating the internal network as potentially compromised, organizations can better defend against both external threats and internal vulnerabilities.

**56.** (A) RPA implementation requires significant changes in infrastructure due to a lack of UI automation capabilities.
Robotic process automation offers several benefits, including the ability to work twenty-four-seven and the generation of full audit trails for compliance. Its drag-and-drop technology allows for workflow automation with minimal coding. Crucially, RPA does not require significant changes to existing infrastructure because it uses user interface automation to interact with legacy systems, making it a highly accessible solution for many banks.

**57.** (A) Its capital intensity makes rural integration a financial challenge.
While 5G technology offers significant advantages in speed and latency, its implementation faces major challenges, particularly regarding capital intensity. The high cost of deploying the necessary infrastructure makes rural integration a significant financial hurdle for service providers. This may lead to a digital divide where urban centers enjoy advanced connectivity while

Click Here to Buy book on Amazon

use. These properties allow money to facilitate commerce and economic planning. While money can take physical forms, its role as a versatile and exchangeable asset is what defines its primary economic utility.

**75.** (D) The system should recover quickly to minimize production impact.
The principle of recoverability in a central bank digital currency system mandates that the network must be able to resume operations quickly after a security breach or technical failure. This ensures that the impact on economic activity is minimized and public confidence in the digital currency is maintained. Robust disaster recovery plans and resilient infrastructure are essential components for achieving this level of operational stability.

**76.** (D) An agile infrastructure that lowers IT costs while remaining scalable.
In the context of fintech, cloud computing is characterized as an agile and scalable infrastructure that helps reduce overall IT costs. It allows financial institutions to deploy resources dynamically based on demand, fostering innovation and faster time-to-market for new services. Unlike legacy on-premise systems, cloud platforms provide the flexibility needed to support modern digital banking applications and large-scale data processing requirements efficiently.

**77.** (A) (I) and (II) only
Offline capabilities in central bank digital currencies allow for transactions without an immediate internet connection. This requires wallets to be able to verify transaction authenticity independently. However, this mode introduces a technical risk of double-spending since the common ledger is not updated in real-time. Therefore, users must eventually synchronize their local wallet balances with the network to ensure the accuracy and integrity of their holdings.

**78.** (D) DBUs offer banking services, including cash deposit and withdrawal, 24x7.
Digital banking units differ from traditional bank branches by providing core services, including cash deposits and withdrawals, on a twenty-four-seven basis. While traditional branches often have limited operating hours and rely on manual paper processing, DBUs utilize automated systems to offer constant accessibility. This model enhances customer convenience and supports the transition toward a more digital and efficient banking environment for all users.

**79.** (B) The central bank issues CBDC through intermediaries to consumers.
The indirect or two-tier model for central bank digital currency issuance involves the central bank creating the digital currency and distributing it through financial intermediaries like commercial banks. These intermediaries are responsible for managing customer accounts, performing identity verification, and handling day-to-day transactions. This approach leverages the existing banking infrastructure and expertise while maintaining the sovereign backing and regulatory oversight of the central bank.

**80.** (D) Digital Rupee (eRupee)
The central bank digital currency issued by the Reserve Bank of India is formally known as the Digital Rupee, often represented as eRupee. This digital form of the national currency is designed to function as legal tender and is backed by the sovereign authority of the state. It represents a significant step in the modernization of India's monetary system and its overall digital payment infrastructure.

**81.** (C) Settlement of secondary market transactions in government securities.
The first pilot for the wholesale digital Rupee, or eRupee-W, focused on the settlement of secondary market transactions in government securities. By using a digital currency for these wholesale activities, the Reserve Bank of India aims to improve efficiency and reduce the time and risk associated with interbank settlements. This specialized application demonstrates the digital currency's potential to transform complex institutional financial markets.

**82.** (D) Assertion (A) is false, but Reason (R) is true.
Digital banking units are designed to deliver financial products in a paperless and efficient digital environment. While they emphasize self-service for tech-savvy users, they are not exclusively restricted to this mode. DBUs also provide an assisted mode where staff can guide

Downloaded from www.pdf.tube

customers through their transactions, ensuring that the technology is accessible to everyone, regardless of their individual level of digital literacy.

**83.** (D) P-4, Q-1, R-3, S-2
Digital banking units offer various features including a self-service mode for independent access and an assisted mode where staff provide guidance to users. These units facilitate end-to-end digital processing for small-ticket retail and MSME loans, significantly reducing paperwork. Furthermore, integration with platforms like the Jan Samarth portal allows for streamlined onboarding to various government-sponsored credit-linked schemes, enhancing financial inclusion efforts.

**84.** (C) They must enforce centralization to restrict ecosystem participation.
Large-scale digital platforms for central bank digital currencies must ensure zero downtime and high transaction volumes to keep the national economy functioning smoothly. They also require robust security features like authentication and data integrity. Contrary to the idea of enforcing centralization to restrict participation, these platforms should be designed to be integrable and accessible to diverse ecosystem participants to foster innovation.

**85.** (C) CBDC appears as an asset on the central bank's balance sheet.
A central bank digital currency is a sovereign currency that is freely convertible into physical cash or commercial bank money. It functions as fungible legal tender and does not strictly require the holder to have a bank account. However, as a form of issued money, it appears as a liability on the central bank's balance sheet, representing an obligation of the issuing monetary authority.

**86.** (B) Private clouds provide increased security to ensure data is not misplaced or lost.
Financial institutions often prefer private clouds for their mission-critical workloads because they provide increased security and control over sensitive data. While public clouds offer great scalability, private environments allow banks to implement customized security protocols and ensure that data is managed in accordance with strict regulatory requirements. This reduced risk of data loss or unauthorized access is vital for maintaining customer trust and operational integrity.

**87.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
It is essential for central bank digital currencies to implement post-quantum cryptographic algorithms to protect against future technological threats. Quantum computers have the potential to process information at speeds far beyond current supercomputers, making traditional encryption methods vulnerable to being broken. By adopting quantum-secure cryptography from the design phase, central banks can ensure the long-term security and resilience of their digital currency systems.

**88.** (B) To improve financial inclusion and management transparency.
The primary objective of deploying digital banking units across the country is to improve financial inclusion and increase the transparency of financial management. These units provide accessible digital banking services to a wide range of citizens, including those in underserved areas. By offering an efficient, paperless, and 24/7 banking environment, DBUs help bring more people into the formal financial system and modernize banking interactions.

NODIA

**89.** (B) P-1, Q-2, R-3, S-4
Central bank digital currencies can take several forms, including token-based systems which function as bearer instruments where the holder is presumed the owner. In contrast, account-based systems require a record of balances and identity verification, which is often performed by intermediaries. These different models offer various balances between anonymity and security, allowing central banks to tailor the digital currency to specific retail or wholesale financial needs.

**90.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Central bank digital currencies serve as a liability of the issuing central bank, similar to physical cash. This is because they are a new variant of central bank money that functions as legal tender

within the existing unit of account. This sovereign backing distinguishes CBDCs from private digital assets, ensuring that they are a stable and trusted medium of exchange for the general public.

**91.** (B) Macro-structured
Big data is typically classified into three primary categories based on its organizational structure: structured data, which resides in fixed formats like databases; unstructured data, which includes diverse formats like video or text; and semi-structured data, which contains some organizational tags. Macro-structured is not a standard term used in data science to describe these primary types of information within analytical frameworks.

**92.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Embedded finance is seen by some traditional financial institutions as a challenge to established banking methods. This is because it allows non-financial enterprises to deliver banking-as-a-service products directly within their own applications. By embedding money and financial tools where consumers already interact, these companies can bypass traditional banking interfaces, potentially changing the way customers engage with and perceive conventional financial service providers.

**93.** (C) CBDC is designed to complement current money as a payment avenue.
According to institutional visions, central bank digital currencies are designed to complement rather than completely replace existing forms of money like physical cash and commercial bank deposits. CBDC provides an additional, modern payment avenue that offers the safety of central bank backing with the efficiency of digital technology. This integrated approach ensures that the monetary system remains resilient and provides diverse options for consumers.

**94.** (C) Indirect model (Two-Tier)
In the scenario where a central bank issues digital currency through commercial banks who then interact with retail consumers, an indirect or two-tier model is being used. Under this system, the central bank maintains its role in settlement and issuance while delegating customer-facing tasks like wallet management and identity verification to intermediaries. This model leverages the strengths of both the public and private financial sectors.

**95.** (B) Chatbots for customers and Robotic Process Automation for back-office entry.
To improve frontline customer interaction and accelerate back-office tasks simultaneously, a bank should implement a combination of chatbots and robotic process automation. Chatbots provide instant, conversational support for customers, while RPA handles repetitive data entry and administrative tasks in the back office with high speed and accuracy. This dual-technology approach enhances overall operational efficiency and improves the quality of service provided to clients.

**96.** (B) CBDC-W (Wholesale)
A digital currency designed specifically for interbank transfers and not accessible to the general public is classified as a wholesale central bank digital currency, or CBDC-W. This type of digital currency is tailored to improve the efficiency of wholesale settlement processes between financial institutions. It aims to reduce settlement risks and lower operational costs in large-scale institutional financial markets without involving everyday retail transactions.

**97.** (D) Transactions can be P2P or P2M via merchant QR codes.
Transactions using the retail digital Rupee can be conducted in two primary ways: person-to-person (P2P) transfers and person-to-merchant (P2M) payments. In the case of merchant transactions, payments are typically made by scanning merchant QR codes at various points of sale. This flexible system allows the digital currency to be used for a wide range of everyday retail activities, mirroring the convenience of current mobile payment methods.

**98.** (A) 5G's primary disadvantage is its universal global coverage in all rural zones.
The global rollout of 5G technology is expected to reach billions of subscriptions by 2025, providing ultra-low latency and high-speed connectivity. While some countries like South Korea adopted the technology early, universal coverage remains a significant challenge. Rural zones, in particular,

Click Here to Buy book on Amazon

**114.** (B) 5G Network
The foundational technology enabler for bringing financial inclusion to remote populations through real-time translation and high-quality virtual reality banking is the 5G network. 5G provides the necessary high bandwidth and ultra-low latency required to support these advanced, data-intensive applications. This connectivity allows individuals in far-off locations to access the same level of sophisticated banking services as those in major urban centers, bridging the digital divide.

**115.** (D) Mandatory reliance on legacy hardware for all infrastructure maintenance
Fintech firms adopting cloud computing expect benefits such as increased scalability, better security-driven innovation, and the agility to adapt quickly to market changes. The cloud allows these companies to move away from expensive on-premise infrastructure. Therefore, any mandatory reliance on legacy hardware for maintaining infrastructure is an exception to these benefits, as the primary goal of cloud adoption is to modernize and streamline IT operations.

**116.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Using offline transactions in a central bank digital currency system introduces a technical risk of double-spending. This is because these transactions occur without instantly updating the common ledger on the central bank's server. Without a real-time record of the transfer, it is possible for a user to attempt to spend the same digital token again before the previous transaction is synchronized and permanently recorded.

**117.** (A) (I), (II), (III), (IV)
When a blockchain processes an asset transfer, the transaction is first logged as a block of data. These blocks then validate the exact timing and sequence of activities. Next, each block is securely linked to those immediately before and after it. Finally, successive blocks reinforce the prior block's verification, creating an immutable and tamper-evident chain that ensures the permanent integrity of the transactional record.

NODIA

**118.** (D) (I), (II), (III), (IV), and (V)
Blockchain functions by logging transactions as data blocks that store specific details like amount and timing. These blocks validate the sequence of events and are linked together securely to prevent historical editing. As more blocks are added, they reinforce the verification of previous ones, making the entire chain tamper-evident. This sequential and decentralized process creates a highly secure and reliable record of all digital asset transfers.

**119.** (A) Robotic Process Automation (RPA)
Robotic process automation is the technology best suited for processing KYC documents by using optical character recognition to read and match data. RPA can handle these repetitive and rule-based tasks with much greater speed and accuracy than human employees. By automating the extraction and entry of information into bank forms, RPA significantly reduces turnaround times and improves overall operational efficiency during the customer onboarding process.

**120.** (A) Account aggregation
Account aggregation is the specific open banking feature that allows a customer to manage multiple financial relationships, such as savings, loans, and investments, from a single mobile application. By consolidating data from various institutions into one view, this feature provides a comprehensive overview of a user's financial health. It simplifies financial management and enables customers to make more informed decisions based on their entire financial portfolio.

**121.** (D) Data segregation and data management
To mitigate security risks when migrating to a public cloud, a financial institution should focus on robust data segregation and data management practices. This best practice ensures that while resources are shared for efficiency, sensitive data remains isolated and protected from unauthorized access. Combined with strict encryption and compliance monitoring, these measures allow banks to enjoy the benefits of cloud scale while maintaining high levels of security and data integrity.

**122.** (C) Product Personalization
When a bank's marketing team uses big data to design specific credit card offers based on

group refers to the specific participants in these pilot projects. Furthermore, double-spending is a technical risk associated with digital tokens where a user might attempt to spend the same unit more than once before the common ledger is updated.

**107.** (A) Scalability issue
When a blockchain network is limited by the number of transactions it can process per second, this is formally referred to as a scalability issue. This limitation can hinder the widespread adoption of public blockchains for high-volume activities like global retail payments. Achieving higher throughput while maintaining decentralization and security is a major focus for developers working on next-generation ledger technologies in the financial sector.

**108.** (A) To foster trust and promote automated agreements via blockchain support.
In the context of 5G and advanced financial technologies, smart contracts play a vital role in fostering trust and promoting automated agreements via blockchain support. These self-executing contracts with the terms directly written into code can trigger actions automatically when specific conditions are met. This reduces the need for manual oversight and can help in creating more transparent and secure transaction frameworks within the banking ecosystem.

**109.** (D) Artificial Intelligence Fraud detection systems
Artificial intelligence fraud detection systems are specifically designed to identify suspicious behavior as it occurs by analyzing massive amounts of real-time data. These systems can recognize patterns and predict future fraudulent activities, allowing banks to intervene immediately. By leveraging location data and transactional habits, AI provides a level of security that far exceeds traditional manual monitoring, protecting both the institution and its customers from financial loss.

**110.** (C) A Consortium Blockchain shares responsibility, while a Private Blockchain is single-governed.
A consortium blockchain is distinguished from a private blockchain primarily by its governance structure. While a private blockchain is controlled and managed by a single organization, a consortium blockchain shares responsibility and decision-making among multiple member organizations. This collaborative approach is often preferred in commercial situations where all parties need to share a common ledger while maintaining a degree of collective control and mutual oversight.

**111.** (D) Cognitive Analytics
Cognitive analytics is the specific technology tailored to handle and extract insights from large, unstructured datasets such as emails, videos, and social media posts. Unlike traditional databases that require structured information, cognitive systems can process these diverse formats without manual pre-tagging. This allows compliance departments and marketing teams to uncover valuable information and patterns that would otherwise be difficult or time-consuming to identify using legacy analytical tools.

**112.** (B) Physical wallets will become entirely obsolete instantly upon the launch of 5G.
The rollout of 5G technology is expected to accelerate the adoption of digital payments, with many consumers already transitioning to mobile-first habits. Additional wearables and internet of things devices will further enhance the appeal of digital wallets. However, the claim that physical wallets will become entirely obsolete instantly upon the launch of 5G is incorrect, as the transition to fully digital societies occurs gradually over time.

**113.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Robotic process automation greatly simplifies the customer onboarding procedure in banks by significantly reducing manual data entry. RPA uses optical character recognition to gather information from KYC documents and then automatically enters it into the relevant client management systems. This automation reduces processing times and eliminates common human errors, resulting in a much faster and more accurate onboarding experience for new bank customers.

Downloaded from www.pdf.tube

**66.** (B) December 1, 2022
The Reserve Bank of India officially launched the first pilot project for the retail digital Rupee on December first, 2022. This initiative, known as eRupee-R, was designed to test the issuance, distribution, and retail usage of a central bank digital currency in a real-world environment. The pilot involved select banks and merchant locations to evaluate the digital currency's functionality and user experience.

**67.** (A) (I) and (II) only
Modern fintech is primarily driven by technologies like artificial intelligence, which provides deep insights into consumer behavior, and big data, which helps forecast market changes. While blockchain is a key driver, its primary value lies in enabling decentralized transactions that reduce the need for traditional third-party intermediaries. Together, these technologies allow financial institutions to develop more efficient, data-driven, and customer-centric business models.

**68.** (B) Issuer, Form, Accessibility, and Technology
Different variants of money are categorized based on four fundamental properties: the issuer, the physical or digital form, the level of accessibility to the public, and the underlying technology used for transactions. These characteristics help distinguish between traditional physical cash, commercial bank deposits, and modern innovations like central bank digital currencies, each offering different levels of security and convenience for users.

**69.** (A) The platform must be decentralized, scalable, and integrable.
The deployment of a central bank digital currency requires a technology platform that is decentralized, scalable, and highly integrable with existing financial systems. This ensures that the digital currency can handle high transaction volumes and work seamlessly across different platforms. The infrastructure must also be designed for maximum uptime and security, providing a reliable and trusted medium of exchange for the entire national economy.

**70.** (C) Providing physical safe deposit locker boxes
Digital banking units provide a wide range of services, including passbook printing, fund transfers, and loan applications. They also facilitate bill payments and tax collections through digital interfaces. However, because DBUs are designed to operate as efficient and paperless digital environments, they typically do not offer traditional physical services like safe deposit locker boxes, which are still primarily found in conventional bank branches.

**71.** (A) Punjab National Bank
The first phase of the retail digital Rupee pilot project involved a select group of financial institutions in India. This group included the State Bank of India, ICICI Bank, and YES Bank, among others. Punjab National Bank was not part of the initial set of banks identified for this specific pilot phase, as the rollout was limited to a small number of participants to ensure controlled testing.

**72.** (B) Cloud services thrive on shared resources, therefore data segregation is heavily discouraged to save costs.
Best practices for cloud adoption in fintech emphasize the importance of discussing encryption policies and ensuring providers have proper compliance certificates. Disaster recovery planning is also a critical requirement for maintaining service continuity. Importantly, data segregation is highly encouraged in shared cloud environments to protect sensitive information, contrary to the idea that it should be avoided to save on operational costs.

**73.** (D) Retail CBDC is meant for restricted access to select institutions.
Central bank digital currencies are classified into retail and wholesale types. Retail CBDC is designed for general public use in everyday transactions, making it available to all citizens. In contrast, wholesale CBDC is intended for restricted access by select financial institutions to facilitate interbank transfers and settlement. Both types aim to improve the efficiency and security of the broader financial and payment ecosystems.

**74.** (A) (I), (II), and (III)
Money serves three primary functions in a modern economy: it acts as a medium of exchange for purchasing goods and services, a unit of account to express value, and a store of value for future

NODIA

individual spending habits, it is primarily illustrating the benefit of product personalization. Big data analytics allows banks to move beyond generic services and create tailored experiences that meet the unique needs of each customer. This approach enhances customer engagement, improves satisfaction, and increases the likelihood that individuals will adopt and use new financial products.

**123.** (C) Account-based CBDC
In a system where an intermediary must verify the identity of an individual before they can utilize a central bank digital currency, an account-based CBDC model is being used. This approach requires maintaining a record of balances and confirming that the person attempting the transaction is the rightful owner of the account. Unlike token-based systems which emphasize bearer-instrument ownership, account-based models rely on formal identification and established digital accounts.

**124.** (A) 5G Network
To provide the ultra-low latency and high bandwidth necessary for advanced applications like instant facial recognition and immersive AR/VR banking, a bank must utilize the 5G network. This next-generation connectivity is essential for delivering seamless, high-definition digital experiences in real-time. By leveraging 5G, banks can transform their physical branches into high-tech hubs that offer interactive and highly personalized services to their customers, significantly improving the overall banking experience.

**125.** (B) By offering services in 'Assisted mode' with staff guidance.
Digital banking units ensure inclusivity by providing an assisted mode specifically for customers who may lack digital literacy or personal computing devices. In this scenario, bank staff are available to guide the customer through their banking transactions, helping them use the digital platform effectively. This approach ensures that the advantages of digital banking are accessible to all citizens, regardless of their technological background or geographic location.

www.nodia.in

Click Here to Buy book on Amazon

network users
(C) Replacing standard alphanumeric passwords with digital signatures
(D) Matching network traffic against a database of known attack patterns or strings

May/June 2018

**45.** Match the ISO 27000 series standards in List I with their primary focus in List II:
List I: (ISO Standard)
P. ISO 27000
Q. ISO 27001
R. ISO 27002
S. ISO 27005
List II: (Primary Focus)
1. Devise framework to implement controls as non-mandatory best practices
2. Build the foundations and establish compliance requirements for ISMS
3. Carry out risk assessment and risk treatment
4. Compilation of international standards related to information security
(A) P-1, Q-3, R-4, S-2
(B) P-2, Q-4, R-3, S-1
(C) P-4, Q-2, R-1, S-3
(D) P-3, Q-1, R-2, S-4

Oct/Nov 2011

**46.** Match the firewall types in List I with their features in List II:
List I: (Firewall Type)
P. Proxy firewalls
Q. NAT firewalls
R. Web application firewalls (WAF)
S. Next-generation firewalls (NGFW)
List II: (Feature)
1. Obscure individual IP addresses to prevent attackers from discovering specific details
2. Defend against application layer web-based attackers via websites
3. Handle deep packet inspection to unpack packet's data
4. Monitor traffic at the OSI model's application layer but speed can be a weakness
(A) P-4, Q-1, R-2, S-3
(B) P-4, Q-1, R-2, S-3
(C) P-1, Q-4, R-3, S-2
(D) P-3, Q-2, R-1, S-4

May/June 2024

**47.** Identify the correct statement representing emerging trends in biometric technology.
(A) Hand-geometry Recognition - Uses ground-based measurements highly sensitive to ambient lighting
(B) Gait Recognition - Identifies individuals based on the way they put one foot in front of another
(C) Vein Recognition - Measures a time dependent correlation of mannerism records
(D) 3D Face Recognition - Evaluates pressure and velocity directly on the writing surface

NODIA

Oct/Nov 2005

**48.** What is a system installed specifically for intruder detection purposes that pretends to be a service but does not advertise itself?
(A) IPSec
(B) Honeypot
(C) LFM
(D) NIPS

May/June 2017

**49.** Voiceprint recognition is based on several acoustic and behavioral factors. Which of the following is NOT a technique or factor utilized in voiceprint recognition?
(A) Measurement of papillary ridges on the vocal cords
(B) Time-history pattern of acoustic strength
(C) Frequency characterization while pronouncing prescribed words
(D) Time dependent correlation and mannerism records

Oct/Nov 2021

**50.** Match the IPS categories in List I with their functions in List II:
List I: (IPS Category)
P. Network-based Intrusion Prevention (NIPS)
Q. Network Behaviour Analysis (NBA)
R. Wireless Intrusion Prevention Systems (WIPS)
S. Host-based Intrusion Prevention Systems (HIPS)
List II: (Function)
1. Examines traffic flow to detect unusual flows which could be results of DDoS
2. Installed as a software package to monitor activities of a single host
3. Monitors the entire network for suspicious activity
4. Analyses wireless networks for suspicious traffic

May/June 2018

**8.** Consider the following statements regarding Smart Cards:

I. They contain a microprocessor or equivalent means of logically processing data.

II. They lack dedicated security logic and internal power.

III. They are self-verifying security cards used in applications like debit and credit cards.

Which of the above statement(s) is/are correct?

(A) Only I and II
(B) Only I and III
(C) Only II and III
(D) I, II, and III

Oct/Nov 2023

**9.** A company wishes to meet compliance regulations by securing access to its core servers. It implements a solution to ensure that database administrators use multi-factor authentication and their activities are logged. Which concept is the company utilizing?

(A) Database Activity Monitoring
(B) Privileged Identity Management
(C) Network Address Translation
(D) Anomaly Detection

May/June 2006

**10.** Why is power supply critical to computing environments even when minor fluctuations are unnoticeable to average users?

(A) They can bypass the internal logical access controls of the primary network
(B) Voltage drops automatically disable critical data encryption protocols
(C) They cause data corruption and loss of service availability
(D) Fluctuations cause automated security entry booths to lock down permanently

Oct/Nov 2014

**11.** Given below are two statements, one labeled as Assertion (A) and the other as Reason (R):

Assertion (A): A server finds it much harder to withstand a DDoS attack compared to a DoS incursion.

Reason (R): DDoS attacks utilize many computers and connections, often distributed globally as part of a botnet, overloading the target with thousands of requests.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2021

**12.** Which type of intrusion detection mechanism uses perimeter detection sensors commonly mounted on fences?

(A) Barrier detectors
(B) Buried-line sensors
(C) Disturbance sensors
(D) Capacitance sensors

NODIA

Oct/Nov 2020

**13.** What is the definition of encryption in data transmission?

(A) Scrambling data at one end of the line, transmitting it, and unscrambling it at the receiver's end
(B) Adding an extra field to a record derived by applying an algorithm agreed between senders and recipients
(C) Filtering data packets arriving from the network router based on IP addresses
(D) Obscuring individual IP addresses by allocating a public address to a group of devices

May/June 2013

**14.** In the context of access control, what is the conceptual distinction between authorization and authentication?

(A) Authorization is the verification of identity, while authentication grants need-based rights
(B) Authorization uses alphanumeric passwords, while authentication uses physical smart cards
(C) Authorization grants rights, while authentication verifies the user's identity
(D) Authorization prevents passive eavesdropping, while authentication prevents active DoS attacks

Oct/Nov 2018

**15.** Match the network threats in List I with their descriptions in List II:

List I: (Network Threat)

P. Impersonation

requiring them to stop at scanners. The system monitors unique physical movement patterns as employees walk down the corridor. Which biometric technology is deployed here?
(A) Gait Recognition
(B) 3D Face Recognition
(C) Vein Recognition
(D) Hand-geometry Recognition

**Oct/Nov 2016**

**58.** Match the Intrusion Detection System methods/types in List I with their functions in List II:
List I: (Detection System Method)
P. NIDS
Q. System integrity verifiers (SIV)
R. Log file monitors (LFM)
S. Anomaly detection
List II: (Function)
1. Monitors system files to find when an intruder changes them
2. Monitors packets on the network wire to discover break-in attempts
3. Measures a baseline of stats and triggers upon deviation
4. Looks for patterns in log files generated by network services
(A) P-2, Q-1, R-4, S-3
(B) P-1, Q-2, R-3, S-4
(C) P-4, Q-3, R-2, S-1
(D) P-3, Q-4, R-1, S-2

**May/June 2012**

**59.** Given below are two statements, one labeled as Assertion (A) and the other as Reason (R):
Assertion (A): Eye Retina Pattern Recognition uses an infrared beam to scan the back of the eye in a circular pattern.
Reason (R): The reflected light is measured by a detector, and correct visual orientation is required for a clear assessment of the pattern.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2019**

**60.** What is the most appropriate description of the difference between an IDS and an IPS?
(A) An IDS actively takes steps to prevent intrusions, whereas an IPS simply logs malicious packets
(B) An IPS actively blocks malicious traffic, while an IDS only detects and logs it
(C) An IDS sits between the firewall and the network, whereas an IPS sits on top of the network layer
(D) An IPS detects statistical anomalies, whereas an IDS exclusively uses signature recognition databases

**May/June 2007**

**61.** Which of the following represents a piece of software that infects programs and data, replicates itself, and can activate upon being triggered by a pre-set condition?
(A) Digital Certificate
(B) Firewall
(C) Virus
(D) VPN

**Oct/Nov 2018**

**62.** What is the most appropriate set of measures for protecting against ransomware?
(A) Regular data backups, OS patching, and updated anti-malware solutions
(B) Utilizing barrier detectors, implementing SIV, and generating user awareness against vishing
(C) Disabling NAT firewalls and segregating data on a single local hard disk partition
(D) Installing keystroke loggers and filtering IP addresses through an enterprise WAF

**May/June 2013**

**63.** A banking institution decides to partner with a third-party technology vendor to host its mobile banking application. The Board initiates a continuous monitoring framework to evaluate the vendor's reliability and security practices. Which Basel Committee principle is being applied here?
(A) Management oversight of outsourcing and third-party vendor relationships
(B) Effective and continuous management oversight of all e-banking activities
(C) Establishment and maintenance of clear audit trails for e-banking transactions
(D) Strategic capacity planning, business continuity, and contingency planning processes

Downloaded from www.pdf.tube

capacitance in near vicinity
(B) Barrier detectors - Send forth a continuous beam of energy
(C) Capacitance sensors - Respond to seismic and magnetic signals
(D) Disturbance sensors - Accomplished through the use of radar

**Oct/Nov 2025**

**23.** An employee traveling for a business meeting leaves a company laptop in a taxi. To ensure that the highly sensitive corporate data stored on it cannot be accessed, which mechanism should have been implemented?
(A) Anchoring pads
(B) Equipment alarm system
(C) Closed Circuit TV
(D) Encryption of information

**May/June 2010**

**24.** Identify the incorrect pair regarding network intrusion types.
(A) Physical Intrusion - Taking apart the system and removing the disk drive
(B) System Intrusion - Intruder already has a low-privilege user account on the system
(C) Remote Intrusion - Intruder attempts to penetrate a system across the network
(D) Remote Intrusion - Intruder begins with extensive administrative privileges

**Oct/Nov 2010**

**25.** Consider the following statements:
I. PIN stands for Personal Identification Number, which identifies a user to a system.
II. In a cash dispenser, the PIN code keyed by the cardholder is matched against the code on the magnetic strip of the card.
Which of the above statement(s) is/are correct?
(A) Only I
(B) Only II
(C) Both I and II
(D) Neither I nor II

**May/June 2005**

**26.** Which of the following is NOT an aspect of physical security?
(A) Intrusion prevention
(B) Document security
(C) Hardware access control
(D) Privileged identity management

NODIA

**Oct/Nov 2022**

**27.** Consider the following threats in a local or wide area network:
I. Impersonation
II. Eavesdropping
III. Data Alteration
IV. Denial of Service (DoS)
Which of the above accurately represent threats that involve tampering with, reading, or faking data rather than simply affecting system availability?
(A) I, II, and III
(B) II, III, and IV
(C) I, III, and IV
(D) I, II, III, and IV

**May/June 2014**

**28.** Which of the following is an incorrect statement regarding document security strategies?
(A) Vital records must be transferred exclusively to USB flash drives for long-term storage
(B) Paper records should be stored in acid-free cardboard cartons or plastic containers
(C) Vital records should be stored at an off-site location away from offices
(D) Periodic reassessments of all vital records should be conducted to ensure they are still valid

**Oct/Nov 2007**

**29.** Given below are two statements, one labeled as Assertion (A) and the other as Reason (R):
Assertion (A): Database Activity Monitoring and Prevention (DAMP) blocks unauthorised activities in real-time.
Reason (R): DAMP is an extension of DAM that not only monitors and sends alerts but is also configured in preventive mode to prevent an actor from carrying out violating activities.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2025**

**30.** Which statement correctly describes the capability of a brute force tool against

Q. Eavesdropping
R. Data Alteration
S. Denial of Service

List II: (Description)

1. Vandalizing to prevent the use of a machine by overloading the CPU
2. Intercepting and reading data by someone other than intended recipients
3. Changing a 'buy' order to a 'sell' order
4. Forging the 'sender' field in an e-mail message

(A) P-3, Q-1, R-4, S-2
(B) P-2, Q-4, R-1, S-3
(C) P-1, Q-3, R-2, S-4
(D) P-4, Q-2, R-3, S-1

**May/June 2007**

**16.** How is the concept of confidentiality defined in the context of computer security?
(A) Only authorized users can access the data resources and information
(B) Only authorized users should be able to modify the data when needed
(C) Data should be available to users when needed
(D) Data must be encrypted during transmission to prevent packet sniffing

**Oct/Nov 2019**

**17.** What conceptually distinguishes system intrusion from remote intrusion?
(A) System intrusion requires a low-privilege account; remote intrusion requires no special access
(B) System intrusion requires physical removal of a disk drive, while remote intrusion requires a user account
(C) System intrusion is executed through a firewall bypass, while remote intrusion uses an IDS
(D) System intrusion relies on spoofed IP addresses, while remote intrusion relies on stolen hardware

**May/June 2012**

**18.** What is the real cost of replacing stolen computers, beyond the cost of the hardware itself?
(A) Rebuilding data and files and replacing lost software
(B) Cost of installing new physical intrusion detection sensors and mechanisms
(C) Cost of purchasing and configuring new uninterruptible power supply systems
(D) Cost of developing and deploying a new organization-wide fire protection plan

**Oct/Nov 2016**

**19.** Match the software security components in List I with their functions in List II:

List I: (Security Component)

P. Smart Cards
Q. DAMP
R. Authentication
S. PIM

List II: (Function)

1. Monitors and blocks unauthorised activities on identified databases
2. Vaults users to ensure servers cannot be accessed by alternate means
3. Makes sure that a message has come from an authorized sender
4. Logically processes data and acts as self-verifying security

(A) P-1, Q-2, R-4, S-3
(B) P-3, Q-4, R-2, S-1
(C) P-2, Q-3, R-1, S-4
(D) P-4, Q-1, R-3, S-2

**May/June 2019**

**20.** Which device monitors the delivery of a one-time password to a coordinating host and prevents observation and re-entry of an intercepted password?
(A) Security Code Generator
(B) Packet-filtering firewall
(C) Disturbance sensor
(D) Smart Card

**Oct/Nov 2009**

**21.** An intruder intercepts a valid electronic transaction intended to purchase shares and modifies the transaction by adding two zeros to the bid amount before forwarding it. What is this network threat called?
(A) DoS
(B) System Intrusion
(C) Data Alteration
(D) Physical Intrusion

**May/June 2023**

**22.** Identify the correct pair regarding intrusion detection mechanisms.
(A) Buried-line sensors - Respond to shifts in

Click Here to Buy book on Amazon

Oct/Nov 2006

**37.** What is the fundamental function of a packet-filtering firewall?
(A) Conducting checks on arriving data packets based on IP, port, and protocol
(B) Opening every data packet to deeply inspect and analyze application-layer contents
(C) Obscuring individual internal IP addresses by allocating a public address to a group
(D) Serving as a bogus bait system installed specifically for early intruder detection

May/June 2016

**38.** Given below are two statements, one labeled as Assertion (A) and the other as Reason (R):
Assertion (A): An IPS can be seen as an extension of an IDS with additional capabilities.
Reason (R): Unlike an IDS, an IPS actively takes steps to prevent intrusions by dropping malicious packets and blocking traffic from malicious IP addresses.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Oct/Nov 2017

**39.** A technology company tests a highly accurate biometric system where data is encoded in a "barcode" format. Which technology is being used?
(A) Retina pattern recognition
(B) Vein recognition
(C) 3D face recognition
(D) Iris pattern recognition

May/June 2008

**40.** Given below are two statements, one labeled as Assertion (A) and the other as Reason (R):
Assertion (A): Honeypots actively take steps to drop malicious packets and block traffic coming from malicious IP addresses.
Reason (R): Programs that pretend to be a service without advertising themselves act as bogus systems to detect intruders, not to actively drop traffic like an IPS.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

NODIA

Oct/Nov 2012

**41.** What is the most appropriate description of the three broad categories of the Basel Committee's risk management principles for e-banking?
(A) Physical site controls, internal network security controls, and biometric access controls
(B) Oversight, security controls, and management of legal and reputational risk
(C) Intrusion prevention systems, data encryption methods, and incident response planning
(D) Customer data privacy, transaction non-repudiation, and overall data integrity standards

May/June 2020

**42.** Which of the following is NOT classified as one of the major types of firewalls based on functioning?
(A) Packet-filtering firewalls
(B) Proxy firewalls
(C) Lures/Honeypots
(D) NAT firewalls

May/June 2011

**43.** Conceptually, why are fingerprints considered highly reliable for biometric verification?
(A) They track the frequency characterization of acoustic strength
(B) They are images of unique papillary ridges in the outer skin layer of fingers
(C) They measure the unique pattern of blood vessels under the skin using infrared light
(D) They capture the three-dimensional image of the hand's geometry

Oct/Nov 2008

**44.** How does signature recognition conceptually operate in intrusion detection?
(A) Detecting statistical anomalies in network traffic without understanding the underlying cause
(B) Monitoring system files to detect unauthorized backdoors left by regular

a 4-character password compared to an 8-character password?
(A) It cracks a 4-character password in 4 seconds and an 8-character password in 4 days
(B) It cracks a 4-character password in 10 seconds and an 8-character password in 4 years
(C) It cracks a 4-character password in 10 years and an 8-character password in 10 decades
(D) It cracks a 4-character password in 4 seconds and an 8-character password in 10 years

**Oct/Nov 2024**

**31.** Consider the following types of network defenses:
I. Packet-filtering firewalls
II. Proxy firewalls
III. NAT firewalls
IV. WAF
V. NGFW
Which of the following combinations comprises the five major types of firewalls segregated based on functioning?
(A) II, III, IV, and V only
(B) I, III, IV, and V only
(C) I, II, III, IV, and V
(D) I, II, III, and IV only

**May/June 2015**

**32.** Consider the following statements about Hand-geometry and Palm-print recognition:
I. Palm-prints have a larger area of operation and more extensive features than fingerprints, making them easier for verification.
II. Hand-geometry recognition operates by measuring a three-dimensional image of the hand.
Which of the above statement(s) is/are correct?
(A) Only I
(B) Both I and II
(C) Only II
(D) Neither I nor II

**Oct/Nov 2013**

**33.** Identify the correct statement regarding Next-generation firewalls (NGFW).
(A) They are considered the most basic type of firewall and do not open data packets.
(B) They can be used in conjunction with software-defined wide area networks (SDWAN).
(C) They operate only at the network routing level without any deep packet inspection capability.
(D) They expose internal individual IP addresses to the public internet intentionally.

**May/June 2011**

**34.** Consider the following statements regarding Face Recognition systems:
I. Traditional 2D face recognition systems are highly sensitive to changes in ambient lighting and view angle.
II. 2D systems are robust against changes in scale, facial accessories, and aging of the user.
III. 3D Face recognition systems solve the ground-based measurement limitations of 2D systems.
Which of the above statement(s) is/are correct?
(A) Only I and II
(B) Only II and III
(C) I, II, and III
(D) Only I and III

**Oct/Nov 2008**

**35.** A network security tool notes that at 2 am, multiple workstations that are normally dormant begin logging into corporate servers and transferring large files. The tool raises an alert based on this deviation. Which detection method is being utilized?
(A) Anomaly detection
(B) Signature recognition
(C) System integrity verification
(D) Network Address Translation

**May/June 2022**

**36.** Identify the correct statement regarding ISO 27001 and ISO 27002 standards.
(A) ISO 27002 was formerly known as ISO 17799 and offers best practices that are not mandatory.
(B) ISO 27002 establishes requirements that are mandatory for certifying an Information Security Management System.
(C) ISO 27001 describes how to implement the controls, whereas ISO 27002 establishes what you have to do.
(D) ISO 27001 is exclusively used for carrying out risk assessment and treatment.

Downloaded from www.pdf.tube

(A) P-4, Q-2, R-1, S-3
(B) P-2, Q-4, R-3, S-1
(C) P-3, Q-1, R-4, S-2
(D) P-1, Q-3, R-2, S-4

**May/June 2009**

**51.** Given below are two statements, one labeled as Assertion (A) and the other as Reason (R):
Assertion (A): An organization must strictly comply with ISO 27002 to certify its Information Security Management System (ISMS).
Reason (R): ISO 27002 provides complex controls, but depending on the context, an organization could implement the control in another way.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2015**

**52.** An organization wants to strictly block data packets containing malicious code specifically targeting its cloud-based application. Which firewall type is typically placed in front of websites to filter such application layer web-based attacks?
(A) Packet-filtering firewall
(B) NAT firewall
(C) Network Behaviour Analysis system
(D) Web application firewall (WAF)

**May/June 2010**

**53.** Identify the correct statement regarding System integrity verifiers (SIV).
(A) Measuring a baseline of CPU utilization to detect distributed denial of service attacks
(B) Actively blocking malicious traffic by dropping packets and resetting IP addresses
(C) Detecting unauthorized system file changes that might indicate a backdoor
(D) Looking for well-known patterns of attack using CGI scripts on a central web-server

**Oct/Nov 2025**

**54.** Match the biometric technologies in List I with their mechanisms in List II:
List I: (Biometric Technology)
P. Vein Recognition
Q. 3D Face Recognition
R. Gait Recognition
S. Voiceprint Recognition
List II: (Mechanism)
1. Uses the way someone walks to identify them
2. Uses infrared light to map blood vessels under the skin
3. Overcomes issues with ambient lighting and facial scale or accessories
4. Develops a time-history pattern of acoustic strength
(A) P-3, Q-1, R-4, S-2
(B) P-4, Q-2, R-3, S-1
(C) P-2, Q-3, R-1, S-4
(D) P-1, Q-4, R-2, S-3

NODIA

**May/June 2023**

**55.** Which of the following is an incorrect statement regarding signature recognition in biometric security?
(A) It relies entirely on the ordinarily discernible pattern of the signature.
(B) Devices operate by signature dynamics, such as history of pressure and velocity.
(C) It takes into account the time, direction, and acceleration of the writing.
(D) Several signatures are needed for initial registration and recognition.

**Oct/Nov 2009**

**56.** Given below are two statements, one labeled as Assertion (A) and the other as Reason (R):
Assertion (A): Speed can be a major weakness of proxy firewalls.
Reason (R): Proxy firewalls monitor traffic at the application layer as an intermediary and utilize stateful and deep packet inspection, which adds extra transfer steps.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2019**

**57.** A high-security facility implements continuous authentication for its employees without

# CHAPTER 15
# Computer Security

**Oct/Nov 2015**

**1.** Match the physical security mechanisms in List I with their characteristics in List II:
List I: (Physical Security Mechanism)
P. Barrier detectors
Q. Buried-line sensors
R. Capacitance sensors
S. Surveillance
List II: (Characteristic)
1. Underground cables sensing pressure, seismic, and magnetic signals
2. Shift in dielectric characteristics triggers corresponding changes
3. Continuous beam of energy
4. Accomplished through radar or CCTV
(A) P-1, Q-2, R-4, S-3
(B) P-4, Q-3, R-1, S-2
(C) P-2, Q-4, R-3, S-1
(D) P-3, Q-1, R-2, S-4

**May/June 2009**

**2.** What does Privileged Identity Management (PIM) primarily focus on?
(A) Monitoring all baseline network traffic deviations across the entire corporate infrastructure
(B) Assigning default passwords to all clerical grade staff members accessing routine programs
(C) Multi-factor authentication and activity logging for powerful infrastructure accounts
(D) Providing biometric verification like fingerprint identification for all banking customers

**Oct/Nov 2021**

**3.** Why is controlling physical access to information systems critical for an organization?
(A) To ensure network packets are filtered before reaching the main servers
(B) To strictly separate the duties of system administrators and database administrators
(C) To prevent unauthorized persons from getting near enough to exploit vulnerabilities
(D) To implement deep packet inspection on physical cables

**May/June 2017**

**4.** Which of the following best describes the main difference between a DoS attack and a DDoS attack?
(A) DoS attacks aim to steal confidential data, whereas DDoS attacks aim to fill up the storage disk
(B) DoS attacks utilize a botnet infrastructure, whereas DDoS attacks utilize a single computer and connection
(C) DoS uses one attacker; DDoS uses many distributed computers to overload a target
(D) DoS attacks bypass proxy firewalls, whereas DDoS attacks bypass Network Address Translation firewalls

**Oct/Nov 2005**

**5.** What is logical security primarily related to?
(A) Automated entry booths and barrier detectors
(B) Software access controls
(C) Power protection and contingency planning
(D) Securing physical hardware from theft

**May/June 2024**

**6.** A competitor secretly intercepts a company's proposal to a bid transmitted over the network without modifying the contents. Which type of network threat does this scenario represent?
(A) Data Alteration
(B) Eavesdropping
(C) Impersonation
(D) Distributed Denial of Service

**Oct/Nov 2011**

**7.** Which of the following defines the prevention of unauthorized data creation, modification, or deletion in computer security?
(A) Confidentiality
(B) Integrity
(C) Availability
(D) Non-repudiation

Click Here to Buy book on Amazon

Oct/Nov 2020

**64.** Which of the following is NOT typically classified as a computer fraud?
(A) Sending hoax emails to scare people
(B) Using spyware to gather information about people
(C) Establishing acid-free containers for paper records
(D) Emailing requests for money in return for "small deposits"

May/June 2021

**65.** Given below are two statements, one labeled as Assertion (A) and the other as Reason (R):
Assertion (A): A logic bomb behaves normally until a certain set of conditions occurs, at which point it maximizes damage.
Reason (R): It can be triggered by events such as a disk becoming nearly full or when a large number of users are using the system.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Oct/Nov 2014

**66.** Given below are two statements, one labeled as Assertion (A) and the other as Reason (R):
Assertion (A): Technical measures alone will fully succeed in a bank marked by staff dissatisfaction and poor supervision.
Reason (R): Surveys show that more than three quarters of frauds are perpetrated by staff of the victim organization.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2006

**67.** Which of the following is NOT one of the principles listed under "Board and Management Oversight" in the Basel Committee's recommendations?
(A) Effective management oversight of e-banking activities
(B) Establishment of a comprehensive security control process
(C) Establishment of clear audit trails for e-banking transactions
(D) Comprehensive due diligence and management oversight process for outsourcing relationships

Oct/Nov 2023

**68.** Given below are two statements, one labeled as Assertion (A) and the other as Reason (R):
Assertion (A): Spoofing and Sniffing are identical techniques used to capture unencrypted data over a network.
Reason (R): Sniffing intercepts and inspects data packets using sniffers, whereas spoofing involves identity impersonation or falsifying data to pretend to be another.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2018

**69.** Consider the following statements:
I. Phishing attacks can be completely eliminated using advanced antivirus checking tools.
II. Only appropriate user education and generating awareness can prevent or reduce the phishing menace.
Which of the above statement(s) is/are correct?
(A) Only II
(B) Only I
(C) Both I and II
(D) Neither I nor II

Oct/Nov 2011

**70.** A bank employee downloads what appears to be a legitimate calculator app. However, while the calculator operates normally, it simultaneously and secretly deletes financial records in the background. What type of malware is this?
(A) Worm
(B) Rootkit
(C) Trojan

Downloaded from www.pdf.tube

Oct/Nov 2023

**116.** A customer conducts an online transaction on their smartphone. Later, they find their confidential card data was stolen from the bank's servers due to a malicious software infection. What type of software facilitates this?
(A) Lebanese loop
(B) Vaccine program
(C) Proxy firewall
(D) Malware

May/June 2018

**117.** Identify the incorrect statement regarding the application of firewalls.
(A) Firewalls establish a secure barrier between a trusted internal network and an untrusted network
(B) NGFWs add critical security functions such as intrusion prevention and anti-malware systems
(C) A WAF focuses on defending against application layer web-based attackers targeting websites
(D) Firewalls remove the need for internal logical access controls like passwords

Oct/Nov 2011

**118.** Consider the following statements regarding Virtual cards:
I. A virtual card is a prepaid card used by infrequent shoppers.
II. It is a limited debit card that provides the primary card information to the merchant and expires after one year.
Which of the above statement(s) is/are correct?
(A) Only II
(B) Both I and II
(C) Neither I nor II
(D) Only I

May/June 2024

**119.** Identify the correct statement regarding Privileged Identity Management (PIM), PUM, and PAM.
(A) They manage server access: who can enter, how they enter, and what they do
(B) PIM focuses on physical barrier detectors, while PUM focuses on system integrity verifiers
(C) They are exclusively used for mitigating distributed denial of service (DDoS) attacks
(D) PAM restricts its scope solely to evaluating the signature dynamics of handwritten signatures

Oct/Nov 2005

**120.** How long does a virtual card typically remain valid before it expires?
(A) A day or 48 hours
(B) One week
(C) A month's grace period
(D) Until the magnetic strip is wiped

May/June 2017

**121.** Identify the incorrect statement regarding Hand-geometry Recognition.
(A) It involves measuring a three-dimensional image of the hand.
(B) It offers several measurable physical characteristics unique to an individual.
(C) It represents a logical step in the biometrical identification process.
(D) Re-enrolment is never required even in case of injury or fingernail length change.

Oct/Nov 2021

**122.** Consider the following statements regarding Lures/Honeypots:
I. They are bogus systems installed for intruder detection purposes.
II. They are programs that pretend to be a service but do not advertise themselves.
III. They can be as complex as an entire subnet of bogus systems installed.
Which of the above statement(s) is/are correct?
(A) Only I and II
(B) Only I and III
(C) I, II, and III
(D) Only II and III

NODIA

May/June 2009

**123.** Consider the following types of computer frauds:
I. Using the computer to solicit minors into sexual alliances
II. Violating copyright laws by copying information with the intent to sell it
III. Hacking into computer systems to gather large amounts of information for illegal purposes
IV. Emails requesting money in return for "small deposits"
Which of the above statement(s) is/are correct?
(A) I, II, and III only
(B) II, III, and IV only

connecting only to trusted Wi-Fi

**Oct/Nov 2025**

**78.** Match the malware types in List I with their descriptions in List II:

List I: (Malware Type)

P. Trojan
Q. Worm
R. Trap door
S. Logic bomb

List II: (Description)

1. Triggered by a certain event, like disk utilization reaching a percentage
2. Undocumented entry-point put in by software developers to bypass access controls
3. Program that survives by copying and replicating itself inside the system from within
4. Program that while visibly performing one function, secretly carries out another

(A) P-4, Q-3, R-2, S-1
(B) P-2, Q-1, R-3, S-4
(C) P-3, Q-4, R-1, S-2
(D) P-4, Q-3, R-2, S-1

**May/June 2023**

**79.** Which of the following is NOT a recommended strategy against viruses or frauds in computing environments?

(A) Ensuring disks received from outside are virus-free before downloading data
(B) Configuring trap doors to automatically delete malicious executables
(C) Clear demarcation between data storage and program storage on separate partitions
(D) Using diskless nodes in a LAN environment

**Oct/Nov 2009**

**80.** A bank customer receives an email that looks exactly like it is from their bank, urging them to click a link and verify their password to prevent account suspension. The goal is to induce the individual to reveal personal information. What is this fraudulent practice called?

(A) Logic bomb
(B) Sniffing
(C) Denial of Service
(D) Phishing

**May/June 2019**

**81.** Banks utilize several measures to deter employees from carrying out fraud. Which of the following combinations of measures helps maintain data integrity and prevent misuse?

I. Division of responsibility
II. Automatic audit trails produced by computer systems
III. Authentication of electronic payments and messages
IV. Validation in computer systems to prevent money being debited to dormant accounts without authorization

Which of the above statement(s) is/are correct?

(A) I, II, and IV only
(B) II, III, and IV only
(C) I, II, III, and IV
(D) I, III, and IV only

**Oct/Nov 2016**

**82.** Consider the following statements regarding Basel Principle 10 of risk management:

I. Banks should have effective capacity, business continuity, and contingency planning processes.
II. These processes are required to help ensure the availability of e-banking systems and services.

Which of the above statement(s) is/are correct?

(A) Both I and II
(B) Only I
(C) Only II
(D) Neither I nor II

**May/June 2012**

**83.** A software vendor installs a new core banking module. Without documentation, the vendor leaves a specific username and password combination hardcoded into the system to bypass standard access controls for future troubleshooting. What is this security risk called?

(A) Rootkit
(B) Trojan
(C) Logic bomb
(D) Trap door (backdoor)

**Oct/Nov 2019**

**84.** An organization discovers that attackers are taking advantage of TCP/IP suite protocols to pretend to be internal users by falsifying IP

Click Here to Buy book on Amazon

III. PureLocker
IV. REvil
V. Tripwire
Which of the above statement(s) is/are correct?
(A) I, II, IV, and V only
(B) I, II, III, and IV only
(C) II, III, IV, and V only
(D) I, III, IV, and V only

**Oct/Nov 2015**

**100.** While shopping on a foreign website, a user decides to input their CVV using a digital keypad on the screen rather than typing it on their physical keyboard. What specific online threat is this precaution designed to avoid?
(A) Pharming
(B) Vishing
(C) Keystroke logging
(D) SIM swipe fraud

**May/June 2010**

**101.** Which of the following is NOT an accepted mechanism of physical intrusion detection?
(A) Anomaly detection
(B) Capacitance sensors
(C) Barrier detectors
(D) Buried-line sensors

**Oct/Nov 2025**

**102.** A fraudster contacts a mobile operator with fake identity proof and obtains a duplicate SIM card, which deactivates the victim's original SIM. The fraudster then generates an OTP to conduct online transactions. What is this fraud called?
(A) SIM swipe fraud
(B) Vishing
(C) Pharming
(D) Card skimming

**May/June 2023**

**103.** What is the most appropriate description of how biometric automation generally operates?
(A) It relies exclusively on complex password hash algorithms to match IP addresses
(B) Converting analogue measurements to digital sequences for reference matching
(C) It maps virtual IP addresses to a corporate network using the PPTP protocol
(D) It encrypts the computer's Master File Table (MFT) until a physical key is presented

**Oct/Nov 2009**

**104.** A customer completes an online purchase and instantly receives an SMS message from their bank detailing the transaction. Which online precaution does this feature represent?
(A) Anti-virus software deployment
(B) Hiding CVV
(C) Using a virtual card
(D) Registering for alerts

**May/June 2019**

**105.** Identify the correct statement concerning a distributed denial of service (DDoS) attack.
(A) It utilizes only one computer and one internet connection to overload a network link.
(B) It relies on guessing the correct password through brute force in 4 seconds.
(C) It utilizes many computers and connections, often distributed as part of a botnet.
(D) It intercepts physical data transmission through buried-line sensors.

NODIA

**Oct/Nov 2016**

**106.** A user at an ATM notices that the keypad feels spongy to the touch and slightly loose. What device is likely placed on top of the actual machine to capture their PIN?
(A) Card skimmer
(B) Fake keypad
(C) False front
(D) Hidden pinhole camera

**May/June 2012**

**107.** What is a limitation of utilizing a vaccine program against computer viruses?
(A) A virus in the bootstrap program can activate before the vaccine loads
(B) The vaccine program requires a hardware smart card to execute successfully
(C) Vaccine programs inevitably trigger logic bombs upon scanning the hard drive
(D) Vaccine programs are incompatible with diskless nodes in a local LAN environment

**Oct/Nov 2019**

**108.** Consider the following online precautions:
I. Shop only on sites that use the 'https' protocol instead of 'http'.
II. Mask CVV with asterisks, especially on foreign websites.
III. Use virtual keyboards to avoid keystroke logging.

(C) I, II, and V only
(D) III, IV, and V only

May/June 2006

**91.** What is the most appropriate reason for avoiding the use of a debit card for e-commerce transactions compared to a credit card?
(A) Debit cards lack EMV chips, making them significantly easier to skim during online use
(B) The risk of instant bank account depletion without a credit grace period
(C) Debit cards cannot be verified using a CVV code on most foreign e-commerce websites
(D) Credit cards automatically block all forms of keystroke logging software by default

Oct/Nov 2023

**92.** Which of the following is NOT a principle categorized under Basel Committee's "Legal and Reputational Risk Management"?
(A) Appropriate disclosures for e-banking services
(B) Privacy of customer information
(C) Proper authorisation controls within e-banking systems
(D) Incident response planning

May/June 2018

**93.** Identify the incorrect pair regarding frauds in online transactions.
(A) Pharming - Fraudsters reroute users to a fake website that seems similar to the original
(B) Keystroke logging - Unintentionally downloaded software that traces key strokes to steal passwords
(C) Public Wi-Fi - Secures transactions completely through automated encryption
(D) Vishing - Identity theft through a mobile phone using voice calls

Oct/Nov 2011

**94.** Which of the following is NOT considered a method of detecting network intrusions?
(A) Anomaly detection
(B) Signature recognition
(C) Non-repudiation and accountability
(D) Network Behaviour Analysis

May/June 2024

**95.** Identify the correct statement regarding the mandate on the security of card transactions by way of EMV chip.
(A) Banks were asked to revert to magnetic stripe cards by September 2017 to improve transaction speed.
(B) Mandating EMV chip and PIN card acceptance enhances safety and facilitates preparedness for the "EMV Liability Shift".
(C) The mandate required ATM card transactions to continue processing exclusively based on data from the magnetic stripe.
(D) POS terminal infrastructure was disabled from accepting EMV chip cards.

Oct/Nov 2005

**96.** Identify the incorrect statement regarding Secure Sockets Layer (SSL) and Transport Layer Security (TLS).
(A) Online shopping should be restricted to sites that are SSL or TLS-certified.
(B) TLS has been replaced by the more secure SSL protocol for all modern e-commerce.
(C) Certified sites can be identified through the lock symbol next to the browser's URL box.
(D) Secure sites use the 'https' protocol where 's' stands for secure.

May/June 2017

**97.** What is the most appropriate description of how the Basel Committee's principle for e-banking disclosure operates in Lebanese loop fraud?
(A) Keystroke logger
(B) Pharming
(C) Phishing
(D) Lebanese loop

Oct/Nov 2021

**98.** Consider the layers of physical security surrounding secure data in an organization:
I. Intrusion Prevention
II. Hardware Access Control
III. Network Access Control
Which of the above statement(s) is/are correct?
(A) I, II, and III
(B) I and II only
(C) II and III only
(D) I and III only

May/June 2009

**99.** Consider the following prominent ransomware attacks:
I. Ryuk
II. Robinhood

Downloaded from www.pdf.tube

# ANSWERS

1. (D) P-3, Q-1, R-2, S-4
Barrier detectors function by emitting a continuous beam of energy to detect interruptions. Buried-line sensors involve underground cables that detect pressure, seismic, or magnetic signals. Capacitance sensors monitor dielectric shifts to trigger alerts. Surveillance is typically achieved through radar or CCTV systems. These mechanisms form a robust physical security framework to protect organizational assets from unauthorized entry or environmental threats.

2. (C) Multi-factor authentication and activity logging for powerful infrastructure accounts
Privileged Identity Management focuses on managing, controlling, and monitoring access to sensitive organizational resources. It involves implementing multi-factor authentication and detailed activity logging for powerful administrative accounts. This ensures that users with elevated permissions are properly verified and their actions are audited to prevent internal misuse. Such controls are essential for protecting core infrastructure from unauthorized or malicious changes.

3. (C) To prevent unauthorized persons from getting near enough to exploit vulnerabilities
Controlling physical access is vital because it prevents unauthorized individuals from gaining close proximity to hardware. When an intruder reaches a system physically, they can exploit vulnerabilities that are otherwise protected by logical security measures. Effective physical controls include barriers, locks, and sensors that safeguard server rooms. This foundational layer of security ensures that only authorized personnel interact with hardware.

4. (C) DoS uses one attacker; DDoS uses many distributed computers to overload a target
Denial of Service attacks involve a single computer attempting to overwhelm a target system. In contrast, Distributed Denial of Service attacks utilize multiple distributed computers, often part of a botnet, to launch coordinated requests. This massive volume of traffic overloads the target's capacity, making it much harder to defend against than a single-source attack. Both aim to disrupt service availability.

5. (B) Software access controls
Logical security refers to the technical measures implemented within software to protect data and systems. It encompasses access controls, encryption, and authentication protocols that manage user permissions. Unlike physical security, which focuses on hardware and premises, logical security ensures that only authorized users can interact with digital information. These software-based protections are critical for maintaining the confidentiality and integrity of electronic assets.

6. (B) Eavesdropping
Eavesdropping involves the unauthorized interception and reading of private communications or data transmissions without altering the content. It is a passive network threat where the attacker gathers sensitive information by listening to traffic. Because the data remains unchanged, the sender and recipient may remain unaware of the breach. This practice highlights the necessity of using encryption to ensure data confidentiality.

7. (B) Integrity
Integrity in computer security ensures that data remains accurate and complete by preventing unauthorized creation, modification, or deletion. It guarantees that information has not been tampered with during storage or transmission. Maintaining integrity is crucial for trust in financial transactions and sensitive records. Organizations use checksums and digital signatures to verify that data is authentic and has not been altered maliciously.

8. (B) Only I and III
Smart cards are advanced security devices containing a microprocessor capable of logically processing data. They are self-verifying and commonly used in financial applications such as credit and debit cards. While they possess

NODIA

IV. Use public Wi-Fi networks for faster identity verification.
V. Register for alerts to receive notifications for online card transactions.

Which of the above statement(s) is/are correct?
(A) I, II, III, and V only
(B) II, III, IV, and V only
(C) I, II, IV, and V only
(D) I, III, IV, and V only

**May/June 2007**

**109.** Consider the following data points inspected by a packet-filtering firewall:
I. Source IP address
II. Destination IP address
III. Port number
IV. Protocol

Which of the above indicate the surface-level data checked to allow or drop packets?
(A) I and II only
(B) II, III, and IV only
(C) I, III, and IV only
(D) I, II, III, and IV

**Oct/Nov 2018**

**110.** Which of the following is an incorrect statement regarding the applicability of the RBI Master Direction on Digital Payment Security Controls?
(A) The directions are applicable to all scheduled commercial banks operating in the region
(B) Small finance banks and Payments banks are bound by these security directions
(C) The directions apply to RRBs and exclude credit card issuing NBFCs
(D) The directions explicitly exclude all Regional Rural Banks (RRBs) from compliance

**May/June 2013**

**111.** Identify the incorrect statement regarding why organizations might not publicly disclose computer frauds.
(A) Many organizations keep such matters secret to avoid public embarrassment.
(B) The banking sector relies on public confidence to attract deposits.
(C) Publicity might have the adverse effect of putting wrong ideas into peoples' minds.
(D) Regulatory authorities prohibit banks from demonstrating effective practices publicly.

**Oct/Nov 2020**

**112.** Which of the following is NOT considered a recommended ATM safeguard?
(A) Watching out for machines that appear to have been altered or look crooked
(B) Entering your PIN twice if an unusual signage commands it to complete the transaction
(C) Covering the keypad with your hand while entering the PIN
(D) Avoiding taking help from any person loitering outside the ATM

**May/June 2021**

**113.** Arrange the following mandates and actions in chronological order:
I. Mandated specific 'digital payment security controls' to be implemented with effect from August 2021.
II. Upgrade of all ATMs with additional safety measures to process EMV chip and PIN cards.
III. Notification for digital payment security controls issued on 18.02.2021.
(A) II, I, III
(B) II, III, I
(C) III, II, I
(D) I, III, II

**Oct/Nov 2014**

**114.** Conceptually, what is the key difference between how biometric signature devices operate versus traditional signature verification?
(A) Biometric devices match the static graphical image rather than how it is written
(B) Biometric devices use writing dynamics, not just the visual signature pattern
(C) Biometric devices require only one signature for registration without averaging characteristics
(D) Biometric devices evaluate fingerprint papillary ridges instead of handwritten pen strokes

**May/June 2006**

**115.** Conceptually, which of the following represents choices available for e-mail encryption?
(A) PPTP and IPsec
(B) BestCrypt and SIV
(C) NIDS and HIPS
(D) PGP and S/MIME

Click Here to Buy book on Amazon

(D) Trap door

May/June 2024

**71.** Match the ATM fraud techniques in List I with their descriptions in List II:
List I: (ATM Fraud Technique)
P. Lebanese loop
Q. Shoulder surfers
R. Card skimmer
S. False front
List II: (Description)
1. Devices installed on the slot to copy the magnetic strip information
2. Small plastic device with a barb that holds the card back in the machine
3. Fake cover that completely covers the original machine, capturing PIN and money
4. People lurking outside or in the ATM room to peer over and read a PIN
(A) P-2, Q-4, R-1, S-3
(B) P-1, Q-3, R-4, S-2
(C) P-4, Q-2, R-3, S-1
(D) P-3, Q-1, R-2, S-4

Oct/Nov 2005

**72.** Conceptually, why does the Basel Committee recommend "Appropriate disclosures for e-banking services" under Legal and Reputational Risk Management?
(A) To ensure appropriate and mandatory segregation of duties within electronic banking systems
(B) To inform customers about the bank's identity and status before transactions
(C) To promote non-repudiation and establish clear accountability for all internal transactions
(D) To authenticate the identity of customers conducting business over the public Internet

May/June 2017

**73.** Arrange the following ransomware-related events in chronological order:
I. CryptoWall accrued over US$18m as ransom money by attackers.
II. WannaCry ransomware attack spread through the Internet infecting lakhs of users.
III. Microsoft issued a "Critical" patch (MS17-010).
(A) I, II, III
(B) I, III, II
(C) III, I, II
(D) II, III, I

Oct/Nov 2021

**74.** Conceptually, what is the primary function of a rootkit?
(A) It redirects users to fake websites.
(B) It monitors keystrokes and transmits them to fraudsters.
(C) It takes root access and replaces system executables.
(D) It intercepts physical ATM card data using an external skimming slot.

May/June 2009

**75.** What is considered a dangerous period where computer fraud can be masked as an error or where security measures are yet to be enforced?
(A) During the deployment of a honeypot
(B) During the implementation of deep packet inspection
(C) During an external regulatory audit
(D) During system development

Oct/Nov 2015

**76.** Consider the following Basel Committee principles related to "Security Controls":
I. Non-repudiation and accountability for e-banking transactions
II. Proper authorisation controls within e-banking systems, databases, and applications
III. Data integrity of e-banking transactions, records, and information
IV. Privacy of customer information
Which of the above statement(s) is/are correct?
(A) I, II, and IV
(B) I, III, and IV
(C) II, III, and IV
(D) I, II, and III

NODIA

May/June 2010

**77.** Identify the correct statement regarding protection against sniffing.
(A) Sniffing is best prevented by ignoring public Wi-Fi networks and ensuring the MFT is deleted
(B) Sniffing requires exploiting the MS17-010 vulnerability to execute remote executables
(C) Sniffing is deterred by categorizing certain messages as spam in standard webmail
(D) Using encryption for important data and

(C) I, II, III, and IV
(D) I, III, and IV only

**Oct/Nov 2015**

**124.** Identify the correct statement concerning VPN connections.
(A) Microsoft includes a technology called PPTP which gives a machine two IP addresses.
(B) IPsec degrades the traditional IP protocol by removing encryption layers.
(C) VPNs operate primarily by creating false IP addresses to spoof an external server.
(D) VPNs cannot be deployed in conjunction with Next-generation firewalls.

**May/June 2010**

**125.** Identify the incorrect statement regarding the features associated with biometric technologies.
(A) Fingerprint Recognition uses papillary ridges in the outer skin layer.
(B) Iris Pattern Recognition relies on discernible writing pattern dynamics.
(C) Vein Recognition uses blood vessel mapping under the skin using infrared light.
(D) Eye Retina Pattern Recognition uses a circular pattern scanned at the back of the eye.

NODIA

www.nodia.in

addresses. To mitigate this spoofing attack, which technical measure should be implemented?
(A) Installing hidden surveillance cameras in the vicinity of the central servers
(B) Migrating all vital records to acid-free cardboard cartons for storage
(C) Using firewalls with deep packet inspection to verify the sender's identity
(D) Implementing a mandatory Master File Table encryption routine for all users

**May/June 2007**

**85.** Which of the following is an incorrect statement regarding ransomware?
(A) It is designed to block access to a computer system until a sum of money is paid.
(B) Advanced malware encrypts the victim's files, sometimes encrypting the computer's Master File Table (MFT).
(C) Wannacry was a ransomware that encrypted files but was easily reversible without a decryption key.
(D) It prevents users from accessing files and acts as a denial-of-access attack.

**Oct/Nov 2018**

**86.** Which of the following is an incorrect statement regarding incident response planning?
(A) It falls under the Legal and Reputational Risk Management category.
(B) It restricts its scope exclusively to capacity planning for physical hardware replacements.
(C) It involves developing plans to manage, contain, and minimise problems arising from unexpected events.
(D) It addresses both internal and external attacks that may hamper the provision of e-banking systems.

**May/June 2013**

**87.** A bank employee discovers a computer fraud perpetrated by an employee but decides to keep the matter secret rather than prosecute publicly. What is a primary reason for an organization to do so?
(A) It significantly reduces the operational burden on internal audit trails and logs
(B) Reputational damage and loss of public confidence in the banking sector
(C) It ensures that the fraudster can be used to test new security detection software
(D) Regulatory authorities mandate complete secrecy for all frauds under US$3 million

**Oct/Nov 2020**

**88.** Identify the correct statement regarding worms in computer security.
(A) A worm requires direct user intervention to copy itself to external data disks
(B) A program that replicates itself inside a computer system without user intervention
(C) A worm's destructive work is obvious and immediate, and it never copies itself
(D) A worm serves as an undocumented entry-point into a high-security computer system

**May/June 2021**

**89.** Consider the following statements regarding protection against viruses:
I. Vaccine programs can deal with widespread varieties, but if the virus lies in the bootstrap program, the virus can work before the vaccine is loaded.
II. Segregation of programs and data on separate hard-disks/partitions increases resistance to viruses.
III. Diskless nodes in a LAN environment are a good protection strategy against viruses.
Which of the above statement(s) is/are correct?
(A) Only I and II
(B) I, II, and III
(C) Only II and III
(D) Only I and III

**Oct/Nov 2014**

**90.** Consider the following definitions related to cyber threats:
I. Spyware: Malware that collects information about users without their knowledge.
II. Phishing: Fraudulent practice of sending emails purporting to be from reputable companies.
III. Email spoofing: Creation of email messages with a forged sender address.
IV. Sniffing: Act of intercepting and inspecting data packets using software or hardware devices.
V. Spamming: Using electronic messaging systems to send unsolicited messages repeatedly.
Which of the above statement(s) is/are correct?
(A) I, II, III, IV, and V
(B) I, II, II, and IV only

Downloaded from www.pdf.tube

dedicated security logic, they rely on an external reader for power. These features make them more secure than traditional magnetic strip cards by providing enhanced authentication and data protection.

9. (B) Privileged Identity Management
Privileged Identity Management is the practice of securing powerful accounts that have elevated access rights within an organization. By requiring database administrators to use multi-factor authentication and logging all their activities, a company can mitigate risks from internal threats or account compromise. This approach ensures accountability and restricts access to core servers to verified users under strictly monitored conditions.

10. (C) They cause data corruption and loss of service availability
Stable power supply is essential for computing environments because even minor voltage fluctuations can lead to severe consequences. These variations can cause immediate data corruption and unexpected loss of service availability, disrupting critical business operations. Reliable power protection systems, such as uninterruptible power supplies, are necessary to safeguard hardware and ensure that background processes and data storage remain consistently operational.

11. (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Servers face significantly greater difficulty defending against Distributed Denial of Service attacks compared to standard Denial of Service incidents. This is because DDoS attacks leverage numerous globally distributed computers, organized as botnets, to flood a target with overwhelming traffic. The distributed nature of these requests makes it nearly impossible to block the source without also impacting legitimate traffic from different locations.

12. (C) Disturbance sensors
Disturbance sensors are specialized intrusion detection mechanisms typically mounted on perimeter fences to detect physical movement or vibrations. When an intruder attempts to climb or cut through a fence, the sensor triggers an alarm based on the mechanical disturbance. These sensors provide an early warning system for physical breaches, allowing security personnel to respond before the intruder reaches sensitive indoor areas.

13. (A) Scrambling data at one end of the line, transmitting it, and unscrambling it at the receiver's end
Encryption is a fundamental process in data transmission that involves scrambling information into an unreadable format using a specific algorithm. The data is transmitted in this secure state and then unscrambled by the authorized recipient who possesses the corresponding key. This mechanism ensures that even if the data is intercepted during transit, it remains confidential and useless to unauthorized parties.

14. (C) Authorization grants rights, while authentication verifies the user's identity
Authentication and authorization are distinct but related security processes. Authentication is the initial step that verifies a user's identity, often through passwords or biometrics. Once the identity is confirmed, authorization determines the specific rights and permissions granted to that user based on their role. This distinction ensures that users only access the resources necessary for their specific job functions.

15. (D) P-4, Q-2, R-3, S-1
Impersonation involves forging identity fields, such as the sender in an email. Eavesdropping is the act of intercepting and reading data intended for others. Data alteration occurs when an attacker changes the contents of a transaction, such as a trade order. Denial of Service is an act of vandalism that overloads a CPU to prevent legitimate system use.

16. (A) Only authorized users can access the data resources and information
Confidentiality is a core principle of computer security that ensures sensitive information is accessible only to authorized individuals. It prevents unauthorized users from viewing or obtaining data that they are not permitted to see. Achieving confidentiality often involves implementing strict access controls, user authentication, and encryption methods. This

NODIA

**51.** (D) Assertion (A) is false, but Reason (R) is true.
An organization is not strictly required to comply with every control in ISO 27002 to certify its Information Security Management System. While ISO 27002 provides a comprehensive set of complex controls, these are intended as best practices. Depending on the specific context and risk assessment, an organization may choose to implement alternative measures that achieve the same security objectives.

**52.** (C) Web application firewall (WAF)
A Web Application Firewall is specifically designed to protect cloud-based applications and websites from application-layer attacks. Unlike traditional firewalls that focus on network traffic, a WAF filters and monitors HTTP traffic between a web application and the internet. This allows it to block malicious code, such as SQL injection or cross-site scripting, before it reaches the core application server.

**53.** (C) Detecting unauthorized system file changes that might indicate a backdoor
System integrity verifiers are essential tools for identifying unauthorized changes to critical system files. By comparing the current state of files against a known-good baseline, an SIV can detect modifications that might indicate the presence of a backdoor or other malicious activity. This monitoring ensures that the fundamental software components of a system remain trustworthy and have not been tampered with.

**54.** (C) P-2, Q-3, R-1, S-4
Vein recognition uses infrared light to map the unique patterns of blood vessels beneath the skin. 3D face recognition overcomes ambient lighting issues by measuring facial depth and scale. Gait recognition identifies individuals by their distinct walking style. Voiceprint recognition analyzes time-history patterns of acoustic strength. These varied mechanisms provide diverse options for secure and accurate biometric authentication in modern systems.

**55.** (A) It relies entirely on the ordinarily discernible pattern of the signature.
Biometric signature recognition is much more sophisticated than simply matching a visual pattern. It does not rely entirely on the discernible appearance of the signature. Instead, the devices monitor signature dynamics, such as the pressure applied, the velocity of the pen, and the acceleration of the writing. This process requires initial registration of several signatures to establish an accurate behavioral baseline.

**56.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Proxy firewalls can experience slower performance because they operate as an intermediary at the application layer. Every data packet must be opened and thoroughly inspected using stateful and deep packet analysis techniques before being passed on. These additional transfer steps and intensive processing requirements create latency, making speed a potential weakness compared to more basic, surface-level packet-filtering firewall systems.

**57.** (A) Gait Recognition
Gait recognition technology identifies individuals by analyzing their unique physical movement and walking patterns. Because it can capture data as employees move naturally down a corridor, it allows for continuous authentication without requiring them to stop at a scanner. This non-intrusive biometric method is ideal for high-security facilities where monitoring the flow of personnel is critical for maintaining overall safety.

**58.** (A) P-2, Q-1, R-4, S-3
Network-based systems monitor packets directly on the wire to find break-in attempts. System integrity verifiers track changes to system files that might indicate an intrusion. Log file monitors look for patterns within the logs generated by various network services. Anomaly detection measures a baseline of statistics and triggers an alert when a significant deviation occurs. These methods provide comprehensive monitoring.

**59.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Eye retina pattern recognition utilizes a low-intensity infrared beam to scan the unique blood vessel patterns at the back of the eye in a circular motion. The intensity of the reflected light is measured by a detector to create a biometric

Click Here to Buy book on Amazon

# STUDYING FROM PDFs?

# THINK AGAIN.

If you are studying only from PDFs,
you are wasting valuable time.

Research shows that learning from

**PRINTED BOOKS** has up to

**4× HIGHER RETENTION**

than studying from screens.

**PRINT BOOK = BETTER MEMORY**

**PDF = LOWER RETENTION**

Those who study from **PRINTED BOOKS**
move **AHEAD.**

Others are left **BEHIND**
in competition.

In competitive exams,
being average is not enough.

## STAY ONE STEP AHEAD.

security measure that ensures the individual using the card is the rightful owner.

**26.** (D) Privileged identity management
Physical security encompasses measures like hardware access control, intrusion prevention systems, and document security. These are designed to protect tangible assets and premises from unauthorized access or damage. In contrast, Privileged Identity Management is a logical security concept focused on managing and monitoring high-level software user accounts. It does not involve the physical protection of hardware or facilities.

**27.** (A) I, II, and III
Network threats such as impersonation, eavesdropping, and data alteration primarily involve the unauthorized reading, tampering, or faking of information. These activities compromise the confidentiality and integrity of data transmissions. While Denial of Service is a significant threat, its main objective is to disrupt system availability rather than manipulate the data itself. Effective security strategies must address all these diverse categories.

**28.** (A) Vital records must be transferred exclusively to USB flash drives for long-term storage
Document security strategies involve the careful preservation and storage of vital records. It is incorrect to assume that transferring such records exclusively to USB flash drives is a sound long-term strategy, as these devices can fail or become obsolete. Proper practices include using acid-free containers, off-site storage, and conducting periodic reassessments to ensure that the records remain valid and accessible.

**29.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Database Activity Monitoring and Prevention systems are designed to detect and block unauthorized activities in real-time. DAMP functions as an advanced extension of basic monitoring by not only alerting administrators to suspicious behavior but also actively preventing users from executing violating actions. This preventive capability is crucial for protecting sensitive databases from both internal misuse and external cyber-attacks.

**30.** (D) It cracks a 4-character password in 4 seconds and an 8-character password in 10 years
The length of a password dramatically impacts its resistance to brute force attacks. A simple four-character password can be compromised in just a few seconds by modern cracking tools. However, increasing the length to eight characters significantly raises the complexity, requiring approximately ten years to crack. This illustrates why organizations mandate longer, complex passwords to protect sensitive user accounts.

**31.** (C) I, II, III, IV, and V
Modern network defense involves various types of firewalls, each serving a specific function. These include packet-filtering firewalls, proxy firewalls, and Network Address Translation systems. Additionally, Web Application Firewalls protect against site-specific attacks, while Next-generation firewalls integrate advanced features like deep packet inspection and intrusion prevention. Together, these technologies form a multi-layered defense strategy for securing corporate network infrastructures.

NODIA

**32.** (B) Both I and II
Palm-print recognition utilizes a larger surface area and more complex features than fingerprints, providing a highly reliable method for individual verification. Similarly, hand-geometry recognition operates by capturing and measuring a three-dimensional image of the hand's shape. Both technologies offer unique biometric characteristics that are difficult to forge, making them suitable for high-security access control systems in various organizations.

**33.** (B) They can be used in conjunction with software-defined wide area networks (SDWAN).
Next-generation firewalls represent an advanced evolution in network security, moving beyond simple packet filtering. They incorporate sophisticated features such as deep packet inspection and integrated intrusion prevention systems. A significant advantage of NGFWs is their compatibility with software-defined wide area networks, allowing organizations to manage security more flexibly across distributed environments while maintaining high levels of protection against threats.

**34.** (D) Only I and III
Traditional 2D face recognition systems often struggle with changes in ambient lighting and viewing angles, which can affect accuracy. Furthermore, these systems are not particularly robust against aging or facial accessories. To overcome these limitations, 3D face recognition technology captures depth-based measurements, providing a more reliable and precise method for identifying individuals regardless of environmental lighting or orientation changes.

**35.** (A) Anomaly detection
Anomaly detection is a method used by security tools to identify suspicious activity by establishing a baseline of normal network behavior. When the system detects a significant deviation from this norm, such as workstations transferring large files during unusual hours, it raises an alert. This approach is effective for identifying new or unknown threats that do not match existing signatures.

**36.** (A) ISO 27002 was formerly known as ISO 17799 and offers best practices that are not mandatory.
The ISO 27000 series provides a framework for information security management. ISO 27002, previously known as ISO 17799, offers a set of best practices and controls that organizations can implement. Importantly, these specific controls are not mandatory for certification. Instead, ISO 27001 establishes the actual requirements for an Information Security Management System that organizations must meet to be certified.

**37.** (A) Conducting checks on arriving data packets based on IP, port, and protocol
A packet-filtering firewall serves as the first line of network defense by examining incoming data packets. It evaluates basic header information, including source and destination IP addresses, port numbers, and protocols, against a set of predefined rules. Based on these checks, the firewall either permits or drops the packets. This process provides an efficient way to block unauthorized traffic.

**38.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
An Intrusion Prevention System is considered an advanced extension of an Intrusion Detection System because it adds proactive response capabilities. While an IDS focuses on monitoring and logging suspicious activity, an IPS takes immediate action to stop potential threats. This includes dropping malicious data packets and blocking traffic from suspicious IP addresses, thereby preventing the intrusion before it causes damage.

**39.** (D) Iris pattern recognition
Iris pattern recognition is a highly accurate biometric technology that analyzes the unique, complex structures of the iris. During the identification process, the system captures an image and encodes the data into a digital format, sometimes referred to as a barcode. This method is exceptionally reliable because iris patterns remain stable over time and are virtually impossible to replicate or forge.

**40.** (D) Assertion (A) is false, but Reason (R) is true.
Honeypots are not designed to actively drop malicious packets or block traffic like an Intrusion Prevention System. Instead, they serve as bogus systems that pretend to be legitimate services to lure and detect intruders. By remaining unadvertised, they act as bait to capture information about attack methods and patterns without interfering with the actual operational network traffic of the organization.

**41.** (B) Oversight, security controls, and management of legal and reputational risk
The Basel Committee established comprehensive risk management principles for electronic banking, categorized into three broad areas. These include management oversight of activities, the implementation of robust security controls, and the management of legal and reputational risks. This framework helps banks ensure the safety and soundness of their digital services while maintaining public confidence and complying with international regulatory standards.

**42.** (C) Lures/Honeypots
Major firewall types classified by their functioning include packet-filtering, proxy, and Network Address Translation firewalls. These systems are designed to filter and manage network traffic to prevent unauthorized access. Lures or honeypots, however, are not firewalls; they are deceptive systems used to detect and study intruders. While

Downloaded from www.pdf.tube

they contribute to security, they do not function as traffic filters or barriers.

**43.** (B) They are images of unique papillary ridges in the outer skin layer of fingers
Fingerprints are highly reliable for biometric verification because they are based on the unique patterns of papillary ridges found on the outer skin layer of the fingers. These patterns are formed before birth and remain virtually unchanged throughout an individual's life. By capturing and matching these distinct ridge details, systems can provide a high degree of accuracy in identifying authorized users.

**44.** (D) Matching network traffic against a database of known attack patterns or strings
Signature recognition in intrusion detection involves comparing network traffic against a comprehensive database of known attack patterns, also known as signatures. When a sequence of data matches a documented threat string, the system identifies it as a malicious attempt and triggers an alert. This method is highly effective for detecting well-known vulnerabilities and exploits that have been previously identified and categorized.

**45.** (C) P-4, Q-2, R-1, S-3
ISO 27000 provides a compilation of international information security standards. ISO 27001 establishes the foundation and compliance requirements for an Information Security Management System. ISO 27002 offers a framework for implementing controls as non-mandatory best practices. ISO 27005 focuses on carrying out risk assessment and treatment. Together, these standards guide organizations in establishing robust security postures and managing risks.

**46.** (B) P-4, Q-1, R-2, S-3
Proxy firewalls monitor traffic at the application layer, though they can experience speed issues. NAT firewalls obscure individual IP addresses to protect network details from discovery. Web application firewalls defend against web-based attacks targeting websites at the application layer. Next-generation firewalls utilize deep packet inspection to analyze the data within packets. These technologies provide layered defense for corporate network security.

NODIA

**47.** (B) Gait Recognition - Identifies individuals based on the way they put one foot in front of another
Gait recognition is an emerging biometric technology that identifies individuals based on their unique walking patterns and physical movement. Unlike systems that require static physical contact or proximity, gait recognition can operate from a distance as a person moves. This makes it useful for continuous authentication in high-security environments without disrupting the flow of authorized personnel through monitored hallways or entrances.

**48.** (B) Honeypot
A honeypot is a security mechanism consisting of a system specifically installed to detect and study intruders. It pretends to be a legitimate service or network resource but is not advertised to regular users. By acting as a decoy, it lures attackers away from critical assets, allowing security professionals to observe their techniques and gather intelligence without risking real data.

**49.** (A) Measurement of papillary ridges on the vocal cords
Voiceprint recognition utilizes a combination of acoustic and behavioral factors to verify an individual's identity. This includes analyzing the time-history pattern of acoustic strength and frequency characteristics during speech. It also considers time-dependent correlations and mannerism records. However, it does not involve measuring papillary ridges, as those are unique characteristics associated with fingerprints rather than the anatomy of vocal cords.

**50.** (C) P-3, Q-1, R-4, S-2
Network-based systems monitor the entire network for suspicious activity. Network Behavior Analysis examines traffic flow to detect unusual patterns, such as those indicating a DDoS attack. Wireless systems focus on identifying suspicious traffic within wireless networks. Host-based systems are software packages installed to monitor activities on a single host. These various categories provide specialized protection across different layers of an organization's infrastructure.

**68.** (D) Assertion (A) is false, but Reason (R) is true.
Spoofing and sniffing are distinct network attack techniques. Sniffing involves the unauthorized interception and inspection of data packets to read unencrypted information. Spoofing, however, is a form of identity impersonation where an attacker falsifies data or addresses to pretend to be a trusted source. While both target network communications, they utilize different methods to compromise security and steal sensitive data.

**69.** (A) Only II
Phishing attacks rely on social engineering to trick individuals into revealing sensitive information. Because these attacks target human behavior rather than just software vulnerabilities, advanced antivirus tools cannot completely eliminate them. The most effective way to prevent or reduce the impact of phishing is through comprehensive user education and generating awareness so that individuals can recognize and avoid fraudulent requests.

**70.** (C) Trojan
A Trojan is a type of malware that disguises itself as a legitimate and useful program, such as a calculator app. While it appears to perform its advertised function normally, it secretly carries out malicious activities in the background, such as deleting financial records or stealing data. Unlike worms or viruses, Trojans do not replicate themselves but rely on deception for installation.

**71.** (A) P-2, Q-4, R-1, S-3
A Lebanese loop uses a small plastic device to trap a card in the machine. Shoulder surfers are individuals who peer over a user's shoulder to read their PIN. Card skimmers are devices installed on the card slot to copy magnetic strip information. A false front is a fake cover that captures both PINs and money. These diverse methods target ATM users.

**72.** (B) To inform customers about the bank's identity and status before transactions
The Basel Committee recommends appropriate disclosures for e-banking services to manage legal and reputational risks. This principle ensures that customers are clearly informed about the bank's identity and regulatory status before they engage in any electronic transactions. Providing such information builds trust and helps prevent fraud by allowing customers to verify that they are dealing with a legitimate financial institution.

**73.** (B) I, III, II
The timeline of major ransomware events began with CryptoWall accruing significant ransom money. Subsequently, Microsoft released the critical MS17-010 patch to address a major vulnerability. Despite this update, the WannaCry ransomware attack later spread rapidly across the internet, infecting hundreds of thousands of users who had not yet applied the patch. This sequence underscores the importance of timely system updates.

**74.** (C) It takes root access and replaces system executables.
A rootkit is a sophisticated type of malware designed to gain administrative, or "root," access to a computer system. Once installed, it often replaces standard system executables with malicious versions, allowing it to remain hidden from users and antivirus software. By controlling the core operating system functions, a rootkit can maintain persistent, unauthorized access while masking its presence and activities.

**75.** (D) During system development
System development is considered a dangerous period for organizations because new code is often being tested and security measures may not yet be fully enforced. During this phase, fraudulent activities can be easily masked as simple errors or bugs. To mitigate this risk, it is essential to implement strict controls and thorough audits throughout the entire software development lifecycle.

**76.** (D) I, II, and III
The Basel Committee's principles for security controls include ensuring non-repudiation and accountability for all e-banking transactions. They also emphasize implementing proper authorization controls within systems, databases, and applications, as well as maintaining the data integrity of all records and information. While protecting customer privacy is also a principle, it is categorized under legal and reputational risk management rather than security controls.

Click Here to Buy book on Amazon

profile. This process requires the user to maintain a specific visual orientation to ensure a clear and accurate assessment.

**60.** (B) An IPS actively blocks malicious traffic, while an IDS only detects and logs it
The fundamental difference between these two systems lies in their response to threats. An Intrusion Detection System is a passive tool that monitors network traffic and logs suspicious activity for review. In contrast, an Intrusion Prevention System is proactive; it not only detects threats but also takes immediate action to block malicious traffic and protect the network from potential damage.

**61.** (C) Virus
A virus is a type of malicious software that attaches itself to programs and data files. It has the ability to replicate itself and spread within a system or across networks. Often, a virus remains dormant until it is triggered by a specific pre-set condition or user action, at which point it can cause significant damage to the infected system.

**62.** (A) Regular data backups, OS patching, and updated anti-malware solutions
Protecting against ransomware requires a multi-layered defense strategy. Maintaining regular data backups ensures that information can be restored without paying a ransom. Applying operating system patches closes vulnerabilities that malware might exploit for entry. Finally, using updated anti-malware solutions provides real-time detection and blocking of malicious software. Together, these measures significantly reduce the risk and impact of ransomware attacks.

**63.** (A) Management oversight of outsourcing and third-party vendor relationships
When a bank partners with a third-party vendor to host its mobile applications, it must apply the Basel Committee principle regarding outsourcing. This involves continuous management oversight to evaluate the vendor's security practices and reliability. Ensuring that third parties meet the bank's safety standards is critical for protecting customer data and maintaining the overall integrity and reputation of the institution.

**64.** (C) Establishing acid-free containers for paper records
Computer fraud encompasses various illegal activities such as sending hoax emails, using spyware for unauthorized information gathering, or soliciting money through deceptive online requests. These actions are intended to cause harm or gain illicit financial benefits. In contrast, establishing acid-free containers for storing paper records is a legitimate and professional document security practice aimed at long-term preservation of physical files.

**65.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
A logic bomb is a type of malicious code that remains dormant and behaves normally within a system until specific conditions are met. Once triggered by events such as a disk reaching a certain capacity or a specific number of users logging in, the code activates to maximize damage. This delayed execution makes it particularly difficult to detect during routine inspections.

**66.** (D) Assertion (A) is false, but Reason (R) is true.
Technical security measures alone are insufficient if a bank suffers from staff dissatisfaction and poor supervision. Research indicates that more than three-quarters of all frauds are perpetrated by internal employees. While software and hardware controls are necessary, they cannot fully protect an organization from malicious insiders who have legitimate access and understand the internal systems and their potential weaknesses.

**67.** (C) Establishment of clear audit trails for e-banking transactions
The Basel Committee's principles for "Board and Management Oversight" include effective management of e-banking activities, establishing security control processes, and conducting due diligence for outsourcing relationships. While establishing clear audit trails is an essential security control, it is categorized under "Security Controls" rather than the specific oversight responsibilities of the board and senior management regarding the broader organizational strategy.

Downloaded from www.pdf.tube

was robust and could not be undone without the specific key held by attackers.

**86.** (B) It restricts its scope exclusively to capacity planning for physical hardware replacements.
Incident response planning is a critical component of legal and reputational risk management. It involves developing comprehensive strategies to contain and minimize problems caused by unexpected internal or external attacks. It is incorrect to claim that its scope is restricted solely to hardware replacement. Instead, it addresses a wide range of security events to ensure the continued provision of e-banking services.

**87.** (B) Reputational damage and loss of public confidence in the banking sector
Organizations, particularly banks, often choose to keep internal frauds secret rather than prosecuting them publicly. A primary reason for this is to avoid significant reputational damage and the potential loss of public confidence. Because the banking sector relies heavily on trust, publicized incidents of employee fraud can discourage deposits and lead to a broader loss of faith in the institution's security.

**88.** (B) A program that replicates itself inside a computer system without user intervention
A worm is a type of malicious software that is characterized by its ability to replicate and spread independently. Unlike a virus, which requires user interaction to infect files, a worm can move across networks and copy itself within a computer system without any intervention from the user. This autonomous nature allows worms to spread rapidly and consume significant system or network resources.

**89.** (B) I, II, and III
Effective protection against viruses involves multiple strategies. Vaccine programs can handle many varieties, though they may be bypassed if a virus activates in the bootstrap program. Segregating programs and data on separate hard disks or partitions also increases resistance. Additionally, using diskless nodes in a local LAN environment is a strong defense, as it prevents users from loading infected software locally.

**90.** (A) I, II, III, IV, and V
Various cyber threats compromise digital security. Spyware gathers user information secretly, while phishing uses deceptive emails to steal data. Email spoofing involves forging sender addresses, and sniffing intercepts data packets for inspection. Spamming refers to sending unsolicited messages repeatedly. Understanding these varied threats is essential for implementing comprehensive security measures to protect individual and organizational data from unauthorized access or misuse.

**91.** (B) The risk of instant bank account depletion without a credit grace period
Using a debit card for e-commerce transactions is generally considered riskier than using a credit card. If a debit card is compromised, funds can be instantly depleted from the linked bank account, leaving the user without immediate access to their money. Credit cards offer a buffer and a grace period, making it easier to dispute fraudulent charges before any actual funds are lost.

**92.** (C) Proper authorisation controls within e-banking systems
The Basel Committee categorizes "Legal and Reputational Risk Management" to include principles such as appropriate disclosures for e-banking services, customer privacy, and incident response planning. However, implementing proper authorization controls within systems is classified under "Security Controls." While authorization is critical for overall security, its focus is on technical access management rather than managing the broader legal or reputational aspects of banking operations.

**93.** (C) Public Wi-Fi - Secures transactions completely through automated encryption
Various techniques are used to commit online fraud, including pharming, keystroke logging, and vishing. These methods target sensitive user data. It is incorrect to claim that public Wi-Fi secures transactions through automated encryption. In fact, public Wi-Fi is often unencrypted and highly insecure, making it easy for attackers to intercept and read data transmitted by unsuspecting users on the network.

NODIA

77. (D) Using encryption for important data and connecting only to trusted Wi-Fi
Protection against sniffing involves measures to prevent unauthorized interception of data packets. The most effective deterrent is the use of strong encryption for all sensitive information, ensuring that even if data is captured, it remains unreadable. Additionally, users should only connect to trusted Wi-Fi networks and avoid public hotspots where attackers can easily monitor and collect unencrypted traffic.

78. (D) P-4, Q-3, R-2, S-1
A Trojan performs one visible function while secretly carrying out another. A worm survives by replicating itself within a system without user intervention. A trap door is an undocumented entry point used to bypass normal access controls. A logic bomb is triggered by a specific event, such as a disk reaching a certain level of utilization. These definitions help identify various threats.

79. (B) Configuring trap doors to automatically delete malicious executables
Recommended strategies for protecting computing environments include verifying that external disks are virus-free, segregating programs and data onto different partitions, and using diskless nodes. These measures help prevent and contain infections. However, it is incorrect to suggest that configuring trap doors is a security strategy. Trap doors are themselves undocumented security risks that provide unauthorized entry into a system.

80. (D) Phishing
Phishing is a fraudulent practice where attackers send deceptive emails that appear to come from reputable sources like banks. These messages often create a sense of urgency to trick recipients into clicking malicious links and revealing sensitive personal information, such as passwords or account numbers. This social engineering tactic is designed to steal credentials and gain unauthorized access to financial accounts.

81. (C) I, II, III, and IV
Banks implement multiple measures to deter internal fraud and maintain data integrity. This includes the division of responsibility among staff and the use of automated audit trails to track system activity. Furthermore, authenticating electronic messages and implementing validation checks to prevent unauthorized debits from dormant accounts are essential. Together, these practices create a robust environment that discourages misuse and ensures accountability.

82. (A) Both I and II
Basel Principle 10 emphasizes that banks must establish effective capacity, business continuity, and contingency planning processes. These measures are necessary to ensure the continuous availability of e-banking systems and services, even during unexpected disruptions. By planning for various scenarios, organizations can minimize downtime and maintain operational resilience, which is critical for preserving customer trust and the stability of the institution.

83. (D) Trap door (backdoor)
A trap door, also known as a backdoor, is an undocumented method for bypassing standard authentication or access controls in a computer system. Developers sometimes leave these hidden entry points for troubleshooting purposes, but if discovered, they pose a significant security risk. Unauthorized individuals can use a trap door to gain full access to the system without being detected by regular logs.

84. (C) Using firewalls with deep packet inspection to verify the sender's identity
To mitigate spoofing attacks where intruders falsify IP addresses to impersonate internal users, organizations should implement advanced firewalls. Systems capable of deep packet inspection can verify the actual identity of the sender beyond simple header information. This technical measure helps ensure that only legitimate, authorized traffic enters the corporate network, effectively blocking malicious attempts to exploit trust based on falsified addresses.

85. (C) Wannacry was a ransomware that encrypted files but was easily reversible without a decryption key.
Ransomware is designed to block access to a computer system or encrypt a victim's files, including the Master File Table, until a ransom is paid. It is incorrect to state that the WannaCry attack was easily reversible without a decryption key. In reality, the encryption used by WannaCry

Click Here to Buy book on Amazon

protection is essential for maintaining the privacy of personal and organizational data.

**17.** (A) System intrusion requires a low-privilege account; remote intrusion requires no special access
System intrusion and remote intrusion differ based on the attacker's starting point. A system intrusion occurs when an individual who already possesses a low-privilege account attempts to gain unauthorized access to more sensitive areas. Remote intrusion involves an attacker with no existing access trying to penetrate a system from across the network. Understanding these differences helps organizations tailor their defenses appropriately.

**18.** (A) Rebuilding data and files and replacing lost software
The true cost of losing stolen computers extends far beyond the physical value of the hardware. Organizations must account for the extensive time and resources required to rebuild lost data, restore critical files, and reinstall software. Additionally, the potential breach of sensitive information can lead to significant operational disruptions. These hidden costs often outweigh the price of a new computer.

**19.** (D) P-4, Q-1, R-3, S-2
Smart cards logically process data and provide self-verifying security features. Database Activity Monitoring and Prevention systems identify and block unauthorized actions on specific databases. Authentication ensures that a received message originates from an authorized sender. Privileged Identity Management utilizes vaulting to ensure that servers are accessed only through authorized means. These components together provide a comprehensive software security layer.

**20.** (A) Security Code Generator
A security code generator is a device that monitors the delivery of one-time passwords to a coordinating host. Its primary function is to prevent the observation and subsequent re-entry of intercepted passwords by unauthorized individuals. By providing a unique, time-sensitive code for each login attempt, it enhances the security of the authentication process and protects against various credential-based attacks.

**21.** (C) Data Alteration
Data alteration is a network threat where an intruder intercepts a valid transaction and modifies its contents before it reaches the recipient. In the context of financial transactions, such as changing a bid amount, this can lead to significant fraudulent gains or losses. This type of attack compromises the integrity of the data and necessitates the use of digital signatures.

**22.** (B) Barrier detectors - Send forth a continuous beam of energy
Barrier detectors are an effective physical security mechanism that function by sending forth a continuous beam of energy across a protected area. When the beam is interrupted by an object or person, the system triggers an alarm. This method is distinct from buried-line sensors that detect seismic signals or capacitance sensors that monitor shifts in near-vicinity electrical fields.

NODIA

**23.** (D) Encryption of information
When sensitive corporate data is stored on a portable device like a laptop, the most effective protection against unauthorized access in case of loss is encryption. Even if the hardware is stolen or misplaced, encrypted information remains unreadable and useless to anyone without the decryption key. This ensures data confidentiality regardless of whether the physical device is recovered by the organization.

**24.** (D) Remote Intrusion - Intruder begins with extensive administrative privileges
Remote intrusion occurs when an attacker attempts to penetrate a system from across a network without having any prior access rights. It is incorrect to state that a remote intruder begins with extensive administrative privileges. Typically, the goal of such an intrusion is to gain initial access and then escalate privileges to perform unauthorized actions or steal sensitive data.

**25.** (C) Both I and II
A Personal Identification Number is a numeric code used to verify a user's identity to a system. In applications like cash dispensers, the PIN entered by the cardholder is matched against the data stored on the card's magnetic strip or chip. This dual-verification process is a standard

**94.** (C) Non-repudiation and accountability
Network intrusion detection involves methods like anomaly detection, signature recognition, and network behavior analysis. These techniques are used to identify and alert administrators to suspicious activities or unauthorized access attempts. Non-repudiation and accountability, however, are security goals related to ensuring that an action cannot be denied by the person who performed it. They are not methods for detecting an intrusion itself.

**95.** (B) Mandating EMV chip and PIN card acceptance enhances safety and facilitates preparedness for the "EMV Liability Shift".
Mandating the use of EMV chip and PIN cards significantly enhances the safety of payment transactions compared to older magnetic stripe technology. This shift provides better protection against card cloning and fraud. Additionally, it ensures that banks are prepared for the "EMV Liability Shift," where the party with the least secure technology becomes responsible for any fraudulent transactions that occur during the process.

**96.** (B) TLS has been replaced by the more secure SSL protocol for all modern e-commerce.
Secure Sockets Layer and Transport Layer Security are protocols used to encrypt communications over the internet. It is incorrect to state that SSL has replaced TLS. In fact, TLS is the more modern and secure successor to SSL. Certified sites using these protocols can be identified by the 'https' prefix and a lock symbol in the browser's address bar, indicating a secure connection.

**97.** (D) Lebanese loop
The Lebanese loop is a specific type of ATM fraud where a perpetrator uses a small plastic device to trap a user's card inside the machine. Once the card is stuck, the criminal often pretends to help, observing the user's PIN. After the user leaves to report the problem, the criminal retrieves the card and uses the stolen PIN to withdraw funds.

**98.** (B) I and II only
Physical security focuses on protecting tangible assets and facilities through layers such as intrusion prevention and hardware access control. These measures include barriers, locks, and sensors to prevent unauthorized physical access to hardware. While network access control is a vital security component, it is a logical measure rather than a physical one, focusing on software-based restrictions for users connecting to the network.

**99.** (B) I, II, III, and IV only
Several prominent ransomware attacks have targeted organizations globally, including Ryuk, Robinhood, PureLocker, and REvil. These malicious programs encrypt files and demand payment for their release. While Tripwire is a well-known name in the security industry, it is a legitimate tool used for monitoring system integrity and detecting changes to files, rather than being a type of malicious ransomware program itself.

**100.** (C) Keystroke logging
Keystroke logging is a threat where malicious software records every key pressed on a physical keyboard to steal sensitive information like passwords and CVV codes. Using a digital keypad on a screen with a mouse or touch input bypasses the physical keyboard entirely. This precaution is specifically designed to prevent keyloggers from capturing the data, ensuring that confidential numbers remain secure.

**101.** (A) Anomaly detection
Physical intrusion detection mechanisms include capacitance sensors, barrier detectors, and buried-line sensors, which are designed to detect unauthorized physical presence or movement. Anomaly detection, however, is a logical security method used to identify suspicious behavior or deviations within network traffic and system usage. It does not involve the physical monitoring of facilities or hardware premises to detect unauthorized entry or proximity.

**102.** (A) SIM swipe fraud
SIM swipe fraud occurs when a criminal uses fraudulent identity documents to convince a mobile operator to issue a duplicate SIM card. This action deactivates the victim's original card, allowing the fraudster to intercept calls and messages. By controlling the phone number, the attacker can receive one-time passwords and conduct unauthorized online transactions using the victim's banking credentials and financial accounts.

Downloaded from www.pdf.tube

(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

May/June 2008

**24.** Which statement is correct regarding the Data Encryption Standard (DES)?
(A) It utilizes variable block sizes ranging from 128 to 256 bits.
(B) It is highly vulnerable to differential cryptanalysis compared to conventional stream ciphers.
(C) It is an asymmetric algorithm used extensively for ATM PIN distribution.
(D) Its most often cited problem today is its relatively short 56-bit key length.

Oct/Nov 2015

**25.** Match the security attributes in List I with their corresponding cryptosystems in List II.
List I: (Security Attributes)
P. Confidentiality and Integrity only
Q. Confidentiality, Integrity, Authentication, and Non-repudiation
R. Single key shared between two entities
S. Public key and private key assigned to an entity
List II: (Cryptosystems)
1. Symmetric Cryptosystem
2. Asymmetric Cryptosystem
3. Symmetric Cryptosystem
4. Asymmetric Cryptosystem
(A) P-3, Q-1, R-4, S-2
(B) P-1, Q-2, R-3, S-4
(C) P-4, Q-2, R-3, S-1
(D) P-2, Q-3, R-1, S-4

May/June 2024

**26.** What term describes a mathematical function utilized specifically for the encryption and decryption processes?
(A) Message digest algorithm
(B) Certificate Revocation List
(C) Hash function
(D) Cryptographic algorithm

Oct/Nov 2006

**27.** In typical 3DES implementations using two conventional DES keys, what is the resulting total key length?
(A) 56 bits
(B) 112 bits
(C) 128 bits
(D) 168 bits

May/June 2012

**28.** Match the cryptographic algorithms in List I with their corresponding categories in List II.
List I: (Algorithms)
P. RSA
Q. AES (Rijndael)
R. ECC
S. Blowfish
List II: (Categories)
1. Symmetric Encryption
2. Asymmetric Encryption
3. Asymmetric Encryption
4. Symmetric Encryption
(A) P-2, Q-1, R-3, S-4
(B) P-1, Q-4, R-2, S-3
(C) P-3, Q-1, R-4, S-2
(D) P-4, Q-2, R-3, S-1

Oct/Nov 2024

**29.** Given below are two statements: one is labelled as Assertion (A) and the other is labelled as Reason (R).
Assertion (A): A key is exactly the same as a passphrase or a password in cryptographic programs.
Reason (R): All possible keys must be equally probable to resist brute-force attacks effectively.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2016

**30.** Which of the following correctly pairs an attribute with its corresponding property in a Symmetric Cryptosystem?
(A) Key length : Variable key length
(B) Speed : Algorithm is more complex and slower
(C) Security Level : Confidentiality, Integrity, Authentication and non-repudiation
(D) Key exchange : Out of band

NODIA

transparency regarding the implementation of security controls.

**112.** (B) Entering your PIN twice if an unusual signage commands it to complete the transaction
ATM safeguards include being vigilant for altered machines, covering the keypad while entering a PIN, and avoiding help from strangers. However, following unusual signage that commands entering a PIN twice is not a safe practice. Such signs are often part of a fraud attempt, such as a Lebanese loop, designed to capture the user's PIN for unauthorized withdrawals later.

**113.** (B) II, III, I
The chronological sequence of these regulatory actions began with the upgrade of ATMs to process EMV chip and PIN cards for enhanced safety. This was followed by the notification issued in February 2021 regarding digital payment security controls. Finally, these specific controls were mandated to be implemented by financial institutions with effect from August 2021, strengthening the overall digital payment ecosystem.

**114.** (B) Biometric devices use writing dynamics, not just the visual signature pattern
Biometric signature verification differs fundamentally from traditional methods by focusing on the process of writing rather than just the final image. These devices measure writing dynamics, including pen pressure, speed, and the specific acceleration used during the signature. By analyzing these behavioral characteristics, the system can more accurately distinguish between an authentic signature and a visually similar forgery.

**115.** (D) PGP and S/MIME
Organizations have several options for securing email communications through encryption. Pretty Good Privacy and Secure/Multipurpose Internet Mail Extensions are two widely recognized standards for this purpose. These protocols ensure that email content and attachments are encrypted before transmission and can only be decrypted by the intended recipient, thereby protecting the confidentiality and integrity of sensitive information during transit.

**116.** (D) Malware
Malicious software, or malware, is a broad category of software designed to infiltrate and damage systems or steal sensitive information. When a bank's servers are infected, malware can capture and transmit confidential card data to unauthorized parties. Protecting against such threats requires a combination of robust firewalls, antivirus software, and regular system monitoring to detect and remove malicious code before it causes harm.

**117.** (D) Firewalls remove the need for internal logical access controls like passwords
Firewalls are essential for creating a secure barrier between trusted and untrusted networks. Next-generation and web application firewalls provide advanced protection against sophisticated threats. However, it is incorrect to believe that firewalls remove the need for internal logical access controls. Even with a firewall in place, organizations must still use passwords, encryption, and other authentication methods to manage internal user access.

**118.** (D) Only I
A virtual card is a secure, prepaid payment option specifically designed for individuals who shop online infrequently. It serves as a digital alternative that protects the user's primary card details from exposure during transactions. However, these cards are typically for single-use or have a very short validity period, such as forty-eight hours, rather than remaining active for an entire year.

**119.** (A) They manage server access: who can enter, how they enter, and what they do
Privileged Identity Management, Privileged User Management, and Privileged Access Management are critical frameworks for securing sensitive systems. They focus on managing high-level server access by controlling who can log in, determining the methods they use for entry, and monitoring their specific activities. This ensures that powerful administrative accounts are strictly audited, reducing the risk of internal misuse or catastrophic data breaches.

**120.** (A) A day or 48 hours
Virtual cards are designed for short-term use to provide maximum security for online

Click Here to Buy book on Amazon

transactions. Unlike traditional physical cards that remain valid for several years, a virtual card typically expires within a very brief window, such as twenty-four or forty-eight hours. This short validity period ensures that the card information cannot be reused by attackers even if it is intercepted.

**121.** (D) Re-enrolment is never required even in case of injury or fingernail length change.
Hand-geometry recognition involves measuring the three-dimensional shape and unique physical characteristics of an individual's hand. While it is a reliable biometric identification process, it is incorrect to state that re-enrolment is never required. Physical changes, such as a significant injury or even a change in fingernail length, can alter the hand's measurements, necessitating a new enrolment to maintain accuracy.

**122.** (C) I, II, and III
Honeypots are bogus systems specifically installed to detect and monitor intruders. They function as programs that pretend to be legitimate services but are not advertised to regular users. These lures can range from a single service to an entire subnet of deceptive systems. By attracting attackers, they provide valuable intelligence on threat patterns while protecting the actual operational network.

**123.** (C) I, II, III, and IV
Computer fraud covers a wide range of illegal activities performed using digital systems. This includes soliciting minors, violating copyright laws for financial gain, and hacking to gather sensitive information for illicit purposes. Additionally, deceptive emails requesting money in exchange for small deposits are common fraudulent practices. All these actions exploit technology to cause harm or achieve unauthorized financial benefits.

**124.** (A) Microsoft includes a technology called PPTP which gives a machine two IP addresses.
Virtual Private Networks are used to create secure connections over untrusted networks. Microsoft utilizes Point-to-Point Tunneling Protocol, which conceptually allows a machine to have two IP addresses: one for the local network and one for the secure tunnel. This technology enables users to access corporate resources securely from remote locations while maintaining the confidentiality and integrity of the data being transmitted.

**125.** (B) Iris Pattern Recognition relies on discernible writing pattern dynamics.
Various biometric technologies use unique physical traits for identification. Fingerprint recognition uses papillary ridges, and vein recognition maps blood vessels using infrared light. Retina pattern recognition scans the back of the eye. However, it is incorrect to state that iris pattern recognition relies on writing dynamics. Iris recognition analyzes the complex structures of the iris, whereas writing dynamics are used in signature verification.

NODIA

www.nodia.in

# CHAPTER 16
# Communication Security

**Oct/Nov 2012**

**1.** Which statement accurately describes symmetric encryption?
(A) The sender encrypts the message with the receiver's public key.
(B) The receiver decrypts the message using a dedicated public key.
(C) The encryption process relies strictly on a variable key length system.
(D) The sender and receiver encrypt and decrypt the message with the same key.

**May/June 2019**

**2.** Evaluate the following statements concerning keys and passphrases:
I A passphrase has significantly less randomness than its length suggests because it needs to be easy to remember.
II Cryptographic programs convert a passphrase into a key through a process called key initialization or hashing.
III To resist an attack, some possible keys must be more probable than others.
Which of the above statement(s) is/are correct?
(A) (I) and (II)
(B) (II) and (III)
(C) (I) and (III)
(D) (I), (II), and (III)

**Oct/Nov 2016**

**3.** In the encryption model, which component is mathematically essential for performing the process of retrieving the original message from the cipher text?
(A) Public registry
(B) Message digest
(C) Decryption key
(D) Certification Authority

**May/June 2007**

**4.** Consider the following statements regarding specific symmetric encryption algorithms:
I 3DES applies the DES algorithm three times to each plaintext block, potentially yielding a key length of 168 bits.
II AES uses key sizes of 128, 192, or 256 bits and was selected through an open competition.
III IDEA is a stream cipher that appeared in 1990 and is less efficient to implement in software than DES.
IV RC4 is a stream cipher that suffers from vulnerability to brute force cracking when a key length of 40 bits or less is used.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (IV)
(B) (II), (III), and (IV)
(C) (I), (III), and (IV)
(D) (I), (II), and (III)

NODIA

**Oct/Nov 2022**

In an asymmetric encryption framework, how is a secure message exclusively read by the intended recipient?
(A) By generating a single out-of-band key shared securely between sender and recipient.
(B) By encrypting with the recipient's public key for decryption via their private key.
(C) By encrypting with the sender's private key and decrypting with the sender's public key.
(D) By using a cryptographic algorithm that hashes the passphrase into a shared symmetric key.

**May/June 2014**

**6.** A system administrator needs to replace legacy DES software with a block cipher that is more efficient in software implementation and offers stronger resistance to differential cryptanalysis. Which algorithm is most appropriate?
(A) RC4
(B) IDEA
(C) RSA
(D) Diffie-Hellman

**Oct/Nov 2005**

**7.** What represents the art and science of keeping files and messages secure by reformatting and

transforming data to make it safer on its trip between computers?
(A) Steganography
(B) Cryptography
(C) Hashing
(D) Encapsulation

**May/June 2011**

**8.** A financial institution decides to implement a bulk encryption mechanism for daily transaction files. Which algorithmic approach is best suited for this requirement?
(A) RSA due to its variable key length and asymmetric nature.
(B) AES (Rijndael) due to algorithm speed and lower complexity.
(C) Diffie-Hellman due to its superior key distribution method and speed.
(D) DSA as it inherently provides efficient bulk file encryption capabilities.

**Oct/Nov 2014**

**9.** What is the process of converting a variable length passphrase into a key?
(A) Obfuscation
(B) Hashing
(C) Steganography
(D) Decapsulation

**May/June 2023**

**10.** Which of the following is not an example of a symmetric encryption algorithm?
(A) Twofish symmetric block cipher
(B) Serpent symmetric block cipher
(C) Diffie-Hellman
(D) Kuznyechik symmetric block cipher

**Oct/Nov 2010**

**11.** For critical applications, which combination of key lengths is specifically indicated as suitable for maintaining security?
(A) 40-bit crypto keys
(B) 56-bit DES and 40-bit RC4
(C) 16-bit IDEA and 32-bit AES keys
(D) 112-bit key 3DES and 128-bit IDEA keys

**May/June 2025**

**12.** How do the two broad classes of symmetric ciphers differ in their operational mechanism?
(A) Stream ciphers use public keys, while block ciphers use private keys.
(B) Stream ciphers are asymmetric, while block ciphers are symmetric.
(C) Stream ciphers work on plaintext one bit at a time, while block ciphers work on groups of bits.
(D) Stream ciphers work on groups of bits, while block ciphers work on plaintext one bit at a time.

**Oct/Nov 2018**

**13.** Why is RSA considered a highly useful cipher despite being much slower than Rijndael?
(A) It offers high scalability for many users, suited for small data like digital signatures.
(B) It handles bulk file encryption more efficiently than high-speed symmetric block ciphers.
(C) It executes single-bit stream cipher operations faster than AES-based implementations.
(D) It employs an out-of-band key exchange mechanism that accelerates network transmissions.

**May/June 2017**

**14.** Given below are two statements: one is labelled as Assertion (A) and the other is labelled as Reason (R).
Assertion (A): Asymmetric encryption algorithms are generally slower than symmetric encryption algorithms.
Reason (R): Asymmetric algorithms use complex mathematical models with variable key lengths, requiring more computational power.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2008**

**15.** Which characteristic distinctly defines the Advanced Encryption Standard (AES)?
(A) It applies the core algorithm three consecutive times to each data block.
(B) It functions as a stream cipher that works on plaintext one single bit at a time.
(C) It utilizes keys of fixed lengths strictly capped at a maximum of 56 bits.
(D) It uses 128-bit blocks and efficient software and hardware implementations.

Downloaded from www.pdf.tube

May/June 2005

**16.** In cryptographic terminology, what is the unencrypted message called before any transformation is applied?
(A) Plaintext
(B) Cipher text
(C) Digest text
(D) Clear key

Oct/Nov 2025

**17.** A longer cryptographic key is always preferable to a shorter key, except in which of the following scenarios where key length does not specifically address the stated condition?
(A) When the key is used exclusively to reduce the speed of network packet routing.
(B) When a single key is used to protect a large number of different messages.
(C) When the information in a message is rarely disclosed except in strictly confidential messages.
(D) When an attacker can do serious damage by recovering and using the crypto key.

May/June 2009

**18.** Which statement regarding asymmetric encryption is incorrect?
(A) The sender encrypts the message using the recipient's private key.
(B) It involves the sender encrypting the message with the receiver's public key.
(C) The receiver decrypts the information using the recipient's private key.
(D) The technique is also known as public key encryption.

Oct/Nov 2007

**19.** What fundamental rule governs the management of private and public keys in an asymmetric algorithm?
(A) The private key is shared via out-of-band mechanisms, while the public key is kept secret.
(B) Both keys must remain strictly confidential and never be broadcasted.
(C) Both keys can be mathematically derived from one another by any third party observing the ciphertext.
(D) The private key must be kept secret by its owner, while the public key may be shared with anyone.

NODIA

May/June 2021

**20.** Which of the following incorrectly pairs an attribute with its corresponding property in an Asymmetric Cryptosystem?
(A) Key length : Fixed key length
(B) Applications : Key encryption and distribution key
(C) Speed : Algorithm is more complex and slower
(D) Key exchange : Public key is encrypted and set with message

Oct/Nov 2011

**21.** Given below are two statements: one is labelled as Assertion (A) and the other is labelled as Reason (R).
Assertion (A): The RC4 cipher is often deployed using a 128-bit key to ensure robust security.
Reason (R): Independent reviews have shown that when RC4 is implemented with key lengths of 40 bits or less, it becomes highly vulnerable to brute force cracking.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2013

**22.** What defines a string of characters used to mathematically encode a message so that it can only be read by someone in possession of an appropriate corresponding element?
(A) Passphrase
(B) Key
(C) Cipher
(D) Hash

Oct/Nov 2021

**23.** Consider the following statements regarding the performance of different encryption techniques:
I The scalability of asymmetric cryptosystems for managing key distribution is far lower than that of symmetric cryptosystems.
II AES (Rijndael) is a symmetric algorithm that was selected to replace DES due to its higher security and efficiency.
Which of the above statements is/are correct?
(A) Only (I)

**103.** (B) Converting analogue measurements to digital sequences for reference matching
Biometric automation operates by capturing unique physical or behavioral characteristics as analogue measurements. These measurements are then converted into precise digital sequences, which are stored as templates. During the verification process, a new scan is compared against the stored digital sequence to determine a match. This method provides a highly reliable and automated way to identify authorized users based on their biological traits.

**104.** (D) Registering for alerts
Registering for alerts is a vital online precaution that allows bank customers to receive instant notifications via SMS or email for every transaction made using their cards. This real-time feature enables users to immediately identify and report any unauthorized or fraudulent activity. By providing constant visibility into account usage, these alerts serve as a critical defense layer for protecting financial assets.

**105.** (C) It utilizes many computers and connections, often distributed as part of a botnet.
A Distributed Denial of Service attack is a coordinated attempt to overwhelm a target network or server. Unlike a standard DoS attack from a single source, a DDoS utilizes a massive number of computers and internet connections, often distributed globally as part of a botnet. This high volume of traffic makes it extremely difficult for the target to maintain availability for legitimate users.

**106.** (B) Fake keypad
A fake keypad is a deceptive device placed directly over the original ATM keypad to capture a user's PIN. If the keypad feels loose or spongy, it may indicate that such a device has been installed. This fraudulent technique allows criminals to record the sequence of buttons pressed by the user, which they then combine with stolen card data to commit fraud.

**107.** (A) A virus in the bootstrap program can activate before the vaccine loads
A significant limitation of vaccine programs is their inability to detect or stop viruses that reside in the system's bootstrap program. Because the bootstrap process occurs during the initial startup phase, a virus located there can activate and take control of the system before the vaccine software has the opportunity to load and begin scanning. This highlights the need for deep-level security.

**108.** (A) I, II, III, and V only
Effective online precautions include shopping only on secure 'https' sites, masking CVV codes on foreign websites, and using virtual keyboards to prevent keystroke logging. Registering for transaction alerts also provides essential real-time monitoring. However, using public Wi-Fi is not a security precaution; rather, it is a risky practice that can expose sensitive information to interception by attackers on the same network.

**109.** (D) I, II, III, and IV
A packet-filtering firewall evaluates several surface-level data points to decide whether to allow or drop traffic. These include the source and destination IP addresses, which identify the sender and receiver. It also checks the port numbers to determine the specific service being accessed and the protocol used for communication. These checks form the basis of initial network access control rules.

**110.** (C) The directions apply to RRBs and exclude credit card issuing NBFCs
The RBI Master Direction on Digital Payment Security Controls applies to commercial banks, small finance banks, and payments banks. It also includes credit card issuing NBFCs. However, the directions explicitly exclude Regional Rural Banks from these requirements. Therefore, suggesting that the directions apply to RRBs while excluding NBFCs is an inaccurate representation of the regulatory framework's actual scope and applicability.

**111.** (D) Regulatory authorities prohibit banks from demonstrating effective practices publicly.
Organizations often maintain secrecy regarding computer frauds to avoid public embarrassment and preserve confidence in the banking sector. Publicity can also unintentionally encourage others to attempt similar crimes. However, it is incorrect to suggest that regulatory authorities prohibit banks from demonstrating effective security practices. On the contrary, regulators often encourage the sharing of best practices and

Click Here to Buy book on Amazon

Oct/Nov 2013

**31.** Given below are two statements: one is labelled as Assertion (A) and the other is labelled as Reason (R).
Assertion (A): A digital signature is unique for each document signed, unlike a handwritten signature which is unique to the signer.
Reason (R): A digital signature is derived from the document itself, meaning any change to the document produces a different digital signature.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2020

**32.** Consider the following statements regarding the legal requirements of digital signatures:
I Authenticity answers whether the message is genuine and identifies the sender.
II Integrity ensures that the document received is complete and unaltered.
III Non-repudiation allows the sender to claim that the contents of the message received are different from what was sent.
IV To establish authenticity during a dispute, a party must retain a record of all relevant messages.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (IV)
(B) (I), (III), and (IV)
(C) (II), (III), and (IV)
(D) (I), (II), and (III)

Oct/Nov 2009

**33.** When considering the theoretical breakability of cipher AES-256 within the context of SSL/TLS across the Internet, what is the most appropriate conclusion?
(A) It is easily crackable due to collision vulnerabilities in the hashing process.
(B) In theory, it is not crackable since the combination of keys is massive.
(C) Breakability is absolute and independent of the technology available at the time.
(D) It suffers from vulnerability to brute force cracking identical to a 40-bit RC4 key.

NODIA

May/June 2006

**34.** What is the most appropriate solution to ensure that a public key in a public database actually belongs to the purported sender?
(A) Distribute private keys securely through trusted manual delivery systems.
(B) Convert the public key into a variable length passphrase for storage.
(C) Encrypt the public key using the intended recipient's private key.
(D) Enlist a Certification Authority to link an entity with the key pair.

Oct/Nov 2017

**35.** Which statement regarding the verification of a digital signature is incorrect?
(A) The program decrypts the digital signature using the sender's private key to extract MD-s.
(B) The recipient's computer runs a program containing the same cryptographic algorithm and hash function used by the sender.
(C) A second message digest (MD-r) is created from the received message.
(D) The recipient verifies message integrity if MD-s and MD-r match perfectly.

May/June 2018

**36.** An organization is deploying a public-key infrastructure. The network administrator highlights the basic issues in secret key management. Which of the following is an underlying goal that must be addressed solely by protecting the secret crypto keys?
(A) Preventing cryptographic services from being used by unauthorized entities.
(B) Distributing public keys in special data blocks across the wide network.
(C) Eliminating the need for any Certification Authority for public distribution.
(D) Converting all block ciphers into stream ciphers for easier key management.

Oct/Nov 2019

**37.** Which of the following statements about 128-bit encryption is incorrect?
(A) It is an asymmetric encryption technique utilizing a public and private key framework.
(B) It is considered one of the most secure encryption methods used in modern encryption algorithms.

(C) It is a data/file encryption technique that uses a 128-bit key to encrypt and decrypt files.
(D) It is considered logically unbreakable as of date.

**May/June 2015**

**38.** Digital signatures satisfy certain legal requirements and business perspectives. Which of the following is not one of these primary requirements?
(A) Authenticity
(B) Integrity
(C) Non-repudiation
(D) Obfuscation

**Oct/Nov 2023**

**39.** What is the fundamental assurance provided by the integrity requirement in a digital communication?
(A) The message source is completely anonymous to third parties.
(B) The sender holds exclusive rights to repudiate the transaction if desired.
(C) The public key has been successfully hidden from public databases.
(D) The document has not been altered either in transmission or storage.

**May/June 2022**

**40.** A corporate manager intends to digitally sign a financial instruction to their bank. To execute this, the manager creates a public-private key pair. Which key will the manager utilize to generate the digital signature for the message?
(A) The bank's public key
(B) The bank's private key
(C) The manager's public key
(D) The manager's private key

**Oct/Nov 2020**

**41.** What is the essential and tricky objective when distributing a public key to ensure its crypto capabilities can be relied upon?
(A) To deliver the public key bundled strictly with the corresponding private key.
(B) To deliver both the public key and the correct name of its owner safely.
(C) To distribute the public key exclusively via an unsecured stream cipher.
(D) To ensure the public key is embedded physically inside the computer's CPU.

**May/June 2010**

**42.** Consider the following statements regarding Message Digest (MD) algorithms:
I MD5 is highly reliable and free from collision problems.
II The SHA-256 algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash.
Which of the above statement(s) is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**Oct/Nov 2012**

**43.** Given below are two statements: one is labelled as Assertion (A) and the other is labelled as Reason (R).
Assertion (A): By successfully decrypting a digital signature, the recipient verifies the authenticity of the message.
Reason (R): Only the sender's public key will decrypt a digital signature that was originally encrypted with the sender's private key.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2019**

**44.** Consider the following statements regarding the verification of a digitally signed message:
I The digital signature is decrypted to yield MD-s.
II A new message digest, MD-r, is generated from the received message.
III If MD-s equals MD-r, the message is considered tampered or altered.
Which of the above statement(s) is/are correct?
(A) (I) and (II)
(B) (II) and (III)
(C) (I) and (III)
(D) (I), (II), and (III)

**Oct/Nov 2016**

**45.** Consider the following statements regarding clients and subjects in Public Key Infrastructure (PKI):

Downloaded from www.pdf.tube

I The client owns the key pair and holds the right to create and change them.
II A subject is granted a license by a CA only to use the key pair.

Which of the above statement(s) is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**May/June 2007**

**46.** Evaluate the following statements concerning cryptographic algorithms and key lengths:
I The likely range of keys for symmetric ciphers will be between 40 and 256 bits.
II 3DES implementations can use three different keys to yield an enormous 168-bit symmetric cipher.
III AES-256 is recommended to be used in SSL/TLS across the Internet.
IV IDEA's underlying mechanism resists differential cryptanalysis better than DES.
V RC4 is a block cipher marketed by RSA Data Security.

Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (IV)
(B) (I), (III), (IV), and (V)
(C) (II), (III), (IV), and (V)
(D) (I), (II), (IV), and (V)

**Oct/Nov 2022**

**47.** An impostor generates a public-private key pair and lists the public key in a directory under a legitimate business owner's name. When a recipient uses this public key to decrypt a digital signature, the process succeeds. Why is this assurance of authenticity worthless?
(A) Because MD-s will naturally fail to match MD-r.
(B) Because the public key belongs to the impostor and not the named sender.
(C) Because symmetric encryption should have been used instead.
(D) Because the message digest was created using a stream cipher instead of a block cipher.

**May/June 2014**

**48.** In the process of creating a digital signature, how is the Message Digest (MD) secured before being sent?
(A) It is encrypted with the recipient's public key.
(B) It is encrypted with the sender's private key.
(C) It is hashed again using SHA-256.
(D) It is encrypted with a symmetric session key.

**Oct/Nov 2005**

**49.** A stockbroker accepts buy/sell orders over the Internet. A client places an order for a volatile forward contract, but the market goes down. The client then attempts to claim they never sent the order. Which digital signature property protects the stockbroker in this scenario?
(A) Non-repudiation
(B) Obfuscation
(C) Integrity
(D) Confidentiality

**May/June 2011**

**50.** During the digital signature verification process, what conclusion is drawn when the decrypted message digest (MD-s) exactly matches the newly generated message digest (MD-r)?
(A) The message came from an impostor who is using a completely bogus public key.
(B) It confirms the message was not altered, verifying its overall integrity.
(C) The sender's private key was compromised during the network transmission process.
(D) The message lacks authenticity and must be rejected as an unverified transmission.

NODIA

**Oct/Nov 2014**

**51.** Which of the following is a correct step in the procedure for generating and delivering secret keys?
(A) Broadcasting the secret key over an unencrypted, out-of-band data channel.
(B) Ensuring keys are easily guessable to prevent administrative user lockout.
(C) Sharing the private key with the Certification Authority for backup storage.
(D) Assign individual keys to the authorized recipients within the database.

**May/June 2023**

**52.** What is the fixed output size generated by the SHA-256 algorithm?
(A) 128-bit (16-byte) hash
(B) 168-bit (21-byte) hash
(C) 256-bit (32-byte) hash
(D) 512-bit (64-byte) hash

(D) RCAI was established to digitally sign the public keys of Certifying Authorities.

**May/June 2008**

**108.** Which statement is correct regarding Export and Import Organizations (EXIM) and the Directorate General of Foreign Trade (DGFT)?
(A) DGFT mandated DSC use with all electronic documents uploaded to their site.
(B) Documents submitted on the DGFT site with a DSC are considered legally inferior.
(C) Only foreign certification authorities can issue DSCs for various DGFT portals.
(D) DGFT prevents EXIM organizations from applying for licenses through online means.

**Oct/Nov 2015**

**109.** Match the symmetric ciphers in List I with their characteristic key properties in List II.
List I: (Symmetric Ciphers)
P. DES
Q. 3DES (two keys)
R. IDEA
S. RC4 (vulnerable state)
List II: (Key Properties)
1. 128-bit key block cipher
2. 40 bits or less
3. 56-bit key length
4. 112 bits length
(A) P-3, Q-4, R-1, S-2
(B) P-1, Q-2, R-3, S-4
(C) P-4, Q-3, R-2, S-1
(D) P-2, Q-1, R-4, S-3

**May/June 2024**

**110.** In very large networks where tens of thousands of users are involved, which type of encryption is most appropriate to use due to its superior scalability?
(A) Symmetric key encryption like DES
(B) Stream cipher encryption like RC4
(C) Public key encryption
(D) Out-of-band key exchange encryption

**Oct/Nov 2006**

**111.** Given below are two statements: one is labelled as Assertion (A) and the other is labelled as Reason (R).
Assertion (A): If a private key is lost, compromised, or no longer used, the corresponding public key and its certificate are placed on the Certificate Revocation List (CRL).
Reason (R): Placing the certificate on the CRL notifies people that they should no longer rely on that key before its expiration date.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2012**

**112.** During online counselling for admission to engineering and medical courses, Digital Signatures are used by the Counselling In-charge. For which specific final action are the choices opted by candidates locked by the invigilators using a Digital Signature Certificate?
(A) Extracting the SHA-256 hash of the student's marksheet.
(B) Choice locking opted by the candidates.
(C) Automatically paying the college tuition fee securely.
(D) Verifying the RC4 encryption of the counselling database.

**Oct/Nov 2024**

**113.** An attacker attempts to decrypt the Aadhaar enrolment data packet intercepted from a client terminal. Assuming the attacker employs millions of computers to break the encryption, what is the expected outcome?
(A) It will be cracked in a matter of weeks using differential cryptanalysis.
(B) The data will naturally expire before it can be broken.
(C) It will take billions of years to break the 2048-bit asymmetric encryption.
(D) The attacker can easily bypass the encryption by forging a MAC address.

**May/June 2016**

**114.** Consider the following statements concerning Certifying Authorities in India:
I The Institute of Development and Research in Banking Technology (IDRBT) is a CA.
II National Informatics Center (NIC) and Tata Consultancy Services (TCS) are prominent CAs.
III The CCA issues digital signature certificates directly for electronic authentication of all

Click Here to Buy book on Amazon

"Who is the sender of the message?" and "Is it a genuine message?"?
(A) Integrity
(B) Non-repudiation
(C) Authenticity
(D) Encapsulation

**May/June 2009**

**60.** A bank receives a digitally signed payment order. The verification software successfully decrypts the signature using the sender's public key but finds that MD-s does not equal MD-r. What action must the recipient take based on this finding?
(A) Accept the message as it verifies non-repudiation and sender authenticity.
(B) Re-encrypt the message digest using the bank's internal private key system.
(C) Reject the message as it indicates the contents were tampered or altered.
(D) Request a manual signature substitute to finalize the payment transaction.

**Oct/Nov 2007**

**61.** Alice wants to validate a certificate signed by a local CA in a hierarchical system. She verifies the local CA's signature, then moves to verify the upper authority's certificate. What is this validation chain ultimately meant to trace back to?
(A) A private key hidden within the sender's browser and local machine.
(B) A variable length passphrase created by the Central Government authority.
(C) A root key or subordinate key received through manual distribution.
(D) The Message Digest of the original plaintext and encrypted metadata.

**May/June 2021**

**62.** What is the most appropriate term for an electronic database of certificates that acts the equivalent of digital Yellow Pages?
(A) Repository
(B) Registration Authority
(C) Root Certifying Authority
(D) Hash Function

**Oct/Nov 2011**

**63.** In the context of a Certification Authority (CA), how is the signature on a certificate verified by a recipient?
(A) By checking it with the CA's public key.
(B) By checking it with the sender's private key.
(C) By checking it with the recipient's private key.
(D) By hashing it with the MD5 algorithm.

**May/June 2013**

**64.** There are typically three parties to a digitally signed electronic communication. Which of the following is incorrectly stated as one of these parties?
(A) The sender of the message who digitally signs it.
(B) The recipient of the message.
(C) The Registration Authority that encrypts the final message payload.
(D) The CA who issues the certificate used by the recipient to verify the digital signature.

**Oct/Nov 2021**

**65.** A banking network requires the integration of cryptographic software to recognize valid certificates. The developer programs the software to check digital signatures attached to certificates. Whose public key must be hard-coded or reliably loaded into this software to perform the check?
(A) The CA's public key
(B) The subscriber's public key
(C) The subscriber's private key
(D) The CA's private key

**May/June 2008**

**66.** Consider the following statements regarding the Internet of Things (IoT) and PKI:
I IoT relies on PKI to play an essential role in a vast number of interconnected applications and devices.
II All network-connected IoT devices require a transparent, consistent form of certificate-based identity authentication.
III The requirements for mobility and IoT are fundamentally different from those of earlier network connected devices.
Which of the above statement(s) is/are correct?
(A) (I) and (II)
(B) (II) and (III)
(C) (I) and (III)
(D) (I), (II), and (III)

Downloaded from www.pdf.tube

Oct/Nov 2010

**53.** Which of the following statements is correct concerning the usage of Digital Signatures?
(A) Private keys are disclosed by posting them in online databases for public use.
(B) Digital signatures serve as a direct physical substitute for an electronic signature.
(C) Public keys are shared via online databases or trusted public repositories.
(D) Senders attach the unencrypted Message Digest directly to the communication.

May/June 2025

**54.** Which of the following incorrectly characterizes the prerequisites for using digital signatures?
(A) The effectiveness depends upon the reliable association of a public-private key pair with an identified person.
(B) An impostor could generate a public-private key pair and enter it under a purported sender's name.
(C) Public-private key pairs have an intrinsic association with a person similar to unique handwriting.
(D) The solution to the association problem is to enlist a trusted third party.

Oct/Nov 2018

**55.** Match the legal requirements of digital signatures in List I with their corresponding definitions in List II.
List I: (Legal Requirements)
P. Authenticity
Q. Integrity
R. Non-repudiation
S. Verification
List II: (Definitions)
1. Holding the sender responsible for his message
2. Confirming the source or origin of a communication
3. Checking if MD-s equals MD-r
4. Ensuring accuracy and completeness of the message
(A) P-2, Q-4, R-1, S-3
(B) P-1, Q-3, R-2, S-4
(C) P-4, Q-2, R-3, S-1
(D) P-3, Q-1, R-4, S-2

May/June 2017

**56.** What is the sequence of bits created by running an electronic message through a one-way hash function called?
(A) Message Digest
(B) Plaintext
(C) Digital Certificate
(D) Passphrase

NODIA

Oct/Nov 2008

**57.** Match the PKI terminology in List I with the descriptions in List II.
List I: (Terminology)
P. PKI
Q. Client
R. Subject
S. Digital Certificates
List II: (Descriptions)
1. The term used by a CA to describe a certificate owner licensed to use a key pair.
2. Signed credentials verified and exchanged within the infrastructure.
3. A framework for secure and trustworthy distribution of public keys.
4. The certificate owner who owns the key pair and has the right to create and change them.
(A) P-3, Q-4, R-1, S-2
(B) P-1, Q-2, R-3, S-4
(C) P-4, Q-3, R-2, S-1
(D) P-2, Q-1, R-4, S-3

May/June 2005

**58.** Consider the following steps involved in sending a message with its Digital Signature:
1. Encrypt the Message Digest with the Sender's Private Key.
2. Run the Message through a Hash Function (Fn-A).
3. Generate the Message Digest (MD-S).
4. Attach the encrypted digital signature to the original message.
Which of the following represents the correct chronological order?
(A) 2, 3, 1, 4
(B) 1, 2, 3, 4
(C) 2, 1, 3, 4
(D) 3, 2, 4, 1

Oct/Nov 2025

**59.** What term is used to describe the requirement that is concerned with the source or origin of a communication, answering questions like

Oct/Nov 2009

**75.** Given below are two statements: one is labelled as Assertion (A) and the other is labelled as Reason (R).
Assertion (A): Public Key Infrastructure meets the increased demand for safe, secure transmission of data in mobile applications and Bring Your Own Device (BYOD) environments.
Reason (R): Mobile certificates are essential in identifying and securing corporate-issued devices as well as supporting mobile payments and cloud services.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2006

**76.** Which statement incorrectly describes the Trusted Manual Distribution of keys?
(A) It is used to distribute the remaining keys that are not distributed via certificates.
(B) Only public keys used for verification of signatures on certificates are distributed this way.
(C) An example is Alice receiving Honest Abe's public key manually through a delivery channel.
(D) It requires manual delivery because the public key's secrecy is critical.

Oct/Nov 2017

**77.** Which statement correctly describes the liability of a Certification Authority (CA)?
(A) A CA operates with absolute immunity and cannot be subject to any claims.
(B) A CA is exclusively liable to the Central Government and holds no liability toward the recipient of a message.
(C) A CA is liable only if they intentionally distribute private keys.
(D) A CA's liability for claims of negligence or misrepresentation may be limited either by law or by contract.

May/June 2018

**78.** Consider the following statements concerning trust models:
I In a centralized system, a signature can grant particular access rights and privileges.
II Hierarchical systems are similar to centralized systems but are more flexible about issuing authorities.
III In web-of-trust systems, a certificate may be signed by several different people.
IV In web-of-trust systems, individuals judge a certificate's meaning based strictly on a single root public key.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (III)
(B) (I), (III), and (IV)
(C) (II), (III), and (IV)
(D) (I), (II), and (IV)

Oct/Nov 2019

**79.** Consider the following statements regarding who can be a Certification Authority:
I In theory, anyone can be a certification authority as long as they are an objective third party with an established reputation for credibility.
II The CA may be assisted by a Registration Authority (RA) to verify the identity of the user.
Which of the above statement(s) is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

May/June 2015

**80.** Bob generates his public key material at his host computer and wishes to obtain a certificate from the CA, Honest Abe. Why is it critical for Bob to choose a reliable means of delivery when copying and delivering his public key to Honest Abe?
(A) Because Honest Abe requires the private key to issue the certificate properly.
(B) Because symmetric encryption requires out-of-band delivery for all participants.
(C) Because the public key will expire immediately if sent over an electronic link.
(D) Because someone might substitute a bogus key or use a different name.

Oct/Nov 2023

**81.** Blockchain technology, including cryptocurrencies like Bitcoin and Ethereum, relies fundamentally on which cryptographic

Click Here to Buy book on Amazon

Oct/Nov 2015

**67.** Evaluate the following statements regarding the contents of a Public Key Certificate:

I It contains the name of the entity.

II It contains the entity's public key.

III It contains a digital signature computed over the name and public key.

Which of the above statement(s) is/are correct?

(A) (I) and (II)
(B) (I) and (III)
(C) (II) and (III)
(D) (I), (II), and (III)

May/June 2024

**68.** Which of the following accurately describes a step in the certification process handled by the subscriber and CA?

(A) The subscriber discloses the private key securely to the CA.
(B) The subscriber generates his/her own public-private key pair.
(C) The CA creates the subscriber's private key and delivers it manually.
(D) The CA encrypts the certificate using the subscriber's private key.

Oct/Nov 2006

**69.** Which statement correctly characterizes the global market for trusted TLS/SSL server certificates?

(A) A few multinational companies hold the market due to technical barriers.
(B) It is highly fragmented with regional providers dominating most of the market.
(C) It is managed by the Root Certifying Authority of India for all global users.
(D) It is monopolized by a single entity that issues every single trusted certificate.

May/June 2012

**70.** Which certificate system model is most appropriate when a system requires the ability to delegate signing certificates through a bureaucratic hierarchy containing multiple layers of CAs?

(A) Web of Trust
(B) Central Authority
(C) Hierarchical Authority
(D) Trusted Manual Distribution

Oct/Nov 2024

**71.** In the Bitcoin blockchain network, a user wants to prove ownership of their funds. Everyone can see their public key. What cryptographic element is kept secret to ensure only the legitimate owner can spend the funds?

(A) The private key
(B) The Certificate Revocation List
(C) The Message Digest hash
(D) The root CA certificate

May/June 2016

**72.** Which of the following is not one of the general types of certificate systems (trust models) utilized to set up the relationship between keys, certificates, authorities, and trust?

(A) Centralized Trust Authority
(B) Random Distribution Authority
(C) Hierarchical Certificate Authority
(D) Global Web of Trust

Oct/Nov 2013

**73.** A digital certificate contains multiple pieces of information ensuring its validity. Which of the following is not typically found within a digital certificate?

(A) The subscriber's public key
(B) An expiration date for the public key
(C) The CA's own digital signature
(D) The subscriber's private key

May/June 2020

**74.** Consider the following statements regarding the validation procedure and certificates:

I A public key certificate is a block of digitally signed data containing a public key and the owner's name.

II An attacker could substitute one public key for another in an exchange if the signature is not checked.

III The certificate's digital signature is produced by the CA.

IV Crypto software must have a copy of the CA's private key to check a certificate's digital signature.

V Software configured properly will reject certificates not issued by the authority it has been trained to recognize.

Which of the above statement(s) is/are correct?

(A) (I), (II), (III), and (V)
(B) (I), (II), (IV), and (V)
(C) (II), (III), (IV), and (V)
(D) (I), (III), (IV), and (V)

NODIA

of the trust chain, certifying the CA Public Keys and issuing certificates.
Reason (R): The Controller of Certifying Authorities (CCA) was appointed by the Central Government under section 18(b) of the Information Technology Act.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2022**

**89.** Match the entities in List I with their corresponding functions in List II.
List I: (Entities)
P. CCA
Q. RCAI
R. RA
S. Symantec
List II: (Functions)
1. The Root Certifying Authority of India established under the IT Act.
2. Appointed by the Central Government to digitally sign the public keys of CAs.
3. Provides the interface between the user and the CA to verify identity.
4. A multinational company dominating the globally trusted TLS/SSL server certificates market.
(A) P-2, Q-1, R-3, S-4
(B) P-1, Q-2, R-4, S-3
(C) P-3, Q-4, R-1, S-2
(D) P-4, Q-3, R-2, S-1

**May/June 2014**

**90.** Match the elements in the validation procedure analogy in List I with their real-world counterparts in List II.
List I: (Analogy)
P. Training of bank tellers
Q. Genuine and forged currency notes
R. Bank tellers rejecting forged notes
S. Forgery test in software
List II: (Real-World Counterparts)
1. Verifying the certificate's digital signature by using the authority's public key
2. Valid and bogus certificates
3. Software rejecting certificates not issued by the recognized authority
4. Providing the CA's public key to crypto software
(A) P-4, Q-2, R-3, S-1
(B) P-1, Q-3, R-2, S-4
(C) P-3, Q-1, R-4, S-2
(D) P-2, Q-4, R-1, S-3

**Oct/Nov 2005**

**91.** Which of the following correctly pairs an Indian digital initiative with its associated benefit or operational feature?
(A) DGFT : Issues physical currency notes endorsed by various digital signatures.
(B) IRCTC : Facilitated online ticketing using DSCs for approved agents.
(C) Aadhaar Data Encryption : Uses DES with 56-bit keys to secure all biometrics.
(D) e-Procurement : Prohibits the use of digital signatures by vendors for tenders.

**May/June 2011**

**92.** Which of the following statements about 3DES is incorrect?
(A) The DES algorithm is applied three times to each plaintext block.
(B) Typical approaches use two conventional DES keys yielding a length of 112 bits.
(C) It is an asymmetric cipher primarily used to establish Web of Trust systems.
(D) It can use three different keys yielding a total key size of 168 bits.

**Oct/Nov 2014**

**93.** What is the most appropriate benefit of using a Digital Signature Certificate with the Ministry of Corporate Affairs (MCA)?
(A) It converts asymmetric encryption into a block cipher format for storage.
(B) It removes the necessity for business houses to file their annual turnover.
(C) It simplifies transactions with the Registrar of Companies and secures data.
(D) It automatically encrypts resident biometrics into various 128-bit key hashes.

**May/June 2023**

**94.** Which of the following is not a step in the certification process performed specifically by the subscriber?
(A) Generates his/her own public-private key pair.

Downloaded from www.pdf.tube

(B) Produces proof of identity, such as a driver's license and passport.
(C) Attaches the CA's own digital signature to the certificate.
(D) Demonstrates that he/she holds the private key corresponding to the public key.

**Oct/Nov 2010**

**95.** What is the most appropriate reason why documents uploaded to the Directorate General of Foreign Trade (DGFT) website with a Digital Signature Certificate are considered on par with physically signed documents?
(A) Because they are encrypted using 3DES algorithms across the entire network.
(B) Because a DSC ensures authenticity and is recognized under the legal system.
(C) Because they are uploaded strictly through a physically secured Intranet terminal.
(D) Because the DGFT website strips away all private keys before accepting any files.

**May/June 2025**

**96.** A utility company integrates smart meters into its network. The security team decides to implement PKI to manage identity authentication. Why is PKI described as the ideal solution for this IoT network?
(A) Because it eliminates the need for a persistent local Internet connection.
(B) It can deliver and manage many certificates at high speed transparently.
(C) Because it forces smart meters to use trusted manual distribution for data.
(D) Because it relies exclusively on 40-bit keys to save metadata bandwidth.

**Oct/Nov 2018**

**97.** Evaluate the following statements regarding Aadhaar Data Encryption:
I Aadhaar enrolment data packets contain resident demographics and biometrics.
II Data is encrypted by the Enrolment Client software at the time of enrolment before saving to disk.
III Encryption uses public key cryptography encryption (PKI-2048 and AES-256).
IV Breaking this encryption would take billions of years even with millions of computers.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (III)
(B) (II), (III), and (IV)
(C) (I), (III), and (IV)
(D) (I), (II), (III), and (IV)

**May/June 2017**

**98.** Consider the following statements regarding Message Digests:
I A Message Digest is a 128 bit length fixed string generated uniquely by SHA-256.
II A Message Digest algorithm acts as a one-way hash function that cannot be decrypted back.
Which of the above statement(s) is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

NODIA

**Oct/Nov 2008**

**99.** Which of the following incorrectly pairs the trust model with its characteristic?
(A) Centralized system : A signature can mean exactly what the central authority wants to mean.
(B) Hierarchical systems : Anyone with a certificate acts exclusively as a single central authority.
(C) Web-of-trust systems : A certificate may be signed by several different people.
(D) Web-of-trust systems : Individuals must judge a certificate's meaning based on personal knowledge of people who signed it.

**May/June 2005**

**100.** Which of the following is not mentioned as a reason or impact of switching to remote work regarding PKI adoption?
(A) The significance and usage of PKI is becoming more visible.
(B) PKI provides the highest level of security and digital trust.
(C) Remote work eliminates the need for Certificate Revocation Lists.
(D) Experts anticipate that the Zero Trust concept will more often be on the "to-implement" list.

**Oct/Nov 2025**

**101.** Consider the following statements regarding eavesdropping prevention and non-repudiation:
I Eavesdropping may be prevented by the use of encryption.

II Non-repudiation means the sender's inability to deny having sent the message.
III Hashing alone is sufficient to legally enforce non-repudiation.
IV Digital signatures satisfy the business perspective requirement of non-repudiation.
Which of the above statement(s) is/are correct?
(A) (I), (II), and (III)
(B) (I), (II), and (IV)
(C) (II), (III), and (IV)
(D) (I), (III), and (IV)

**May/June 2009**

**102.** Which statement incorrectly describes the usage of Digital Signatures in e-Procurement in India?
(A) Officials use digital signatures while vendors are limited to physical ones.
(B) e-Procurement is an online tender processing system for state government departments.
(C) More than 1000 tenders have been published so far through this electronic system.
(D) Vendors and traders use Digital Signatures for applying to tenders on the internet.

**Oct/Nov 2007**

**103.** Which statement is correct regarding the International Data Encryption Algorithm (IDEA)?
(A) It is less efficient to implement in software than DES or 3DES.
(B) Its underlying mechanism resists differential cryptanalysis better than DES.
(C) It uses a 56-bit key, making it highly vulnerable to brute force cracking.
(D) It is an asymmetric algorithm marketed by RSA Data Security.

**May/June 2021**

**104.** Evaluate the following statements regarding the current status and future of Public Key Infrastructure (PKI):
I The technology itself has withstood close scrutiny by countless experts over the past forty years.
II User confidence in the effectiveness of PKI is stronger than ever.
III PKI remains the most practical and cost-effective solution to growing security challenges.
IV Cryptography ensures security of messages in the communication environment.
V Certification Authorities distribute keys to the participants of electronic communication.
Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (IV)
(B) (II), (III), (IV), and (V)
(C) (I), (III), (IV), and (V)
(D) (I), (II), (III), (IV), and (V)

**Oct/Nov 2011**

**105.** Which of the following is not cited as a driver for the growth of mobile certificates and Public Key Infrastructure (PKI)?
(A) Secure mobile connection to high-speed corporate Wi-Fi and VPN networks.
(B) Facilitating secure mobile payment gateways and diverse cloud services.
(C) Reducing AES block size to 56 bits for faster mobile packet routing.
(D) Identifying and securing Bring Your Own Device (BYOD) corporate environments.

**May/June 2013**

**106.** Given below are two statements: one is labelled as Assertion (A) and the other is labelled as Reason (R).
Assertion (A): E-Filing of Tax Returns is mandatory for all individuals or professionals having an annual gross receipt of INR 50 Lakhs and above.
Reason (R): Revised provisions under section 44AB of the IT Act enforce the mandatory use of Digital Signature Certificates for E-Filing at these specific thresholds.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2021**

**107.** Which statement is incorrect regarding the legal foundation of Certifying Authorities in India?
(A) The IT Act prohibits digital signatures for firms above 1 Crore turnover.
(B) The CCA is appointed by the Central Government to oversee the PKI system.
(C) RCAI is established under the specific terms of the Information Technology Act.

Click Here to Buy book on Amazon

concept for identity management and transaction authentication?
(A) Symmetric cryptography
(B) Steganography
(C) Asymmetric cryptography
(D) Trusted Manual Distribution

**May/June 2022**

**82.** In a Hierarchical Authority system, whose certificate must an individual user validate to trace the chain back to a key received through manual distribution?
(A) The immediate local CA that signed the user's certificate.
(B) The peer user's private key and associated message digest.
(C) Only the final recipient's public key and registration data.
(D) The Registration Authority's private key and security token.

**Oct/Nov 2020**

**83.** Which statement correctly identifies some of the prominent Certifying Authorities (CAs) operating in India?
(A) Only multinational corporations like Symantec and GoDaddy operate as CAs in India.
(B) The Registration Authority (RA) is the sole CA allowed under the IT Act 2000.
(C) RCAI operates as the only commercial CA issuing digital signatures directly to end-users.
(D) IDRBT, NIC, TCS, NSDL, and CDAC are certifying authorities in India.

**May/June 2010**

**84.** A company discovers that an employee's private key has been compromised. The certificate has not yet reached its expiration date. What mechanism should the CA use to notify people that they should no longer rely on this key?
(A) Issue a new private key to overwrite the old one across all server nodes.
(B) Change the algorithm from RSA to AES to prevent further data decryption.
(C) Place the corresponding public key and its certificate on the CRL.
(D) Broadcast the compromised private key globally to warn all potential users.

**Oct/Nov 2012**

**85.** Which statement incorrectly details the requirements a subscriber must fulfill when interacting with a Certification Authority (CA)?
(A) The subscriber produces proof of identity, such as a driver's license or passport.
(B) The subscriber contacts the CA either in person or through an online portal.
(C) The subscriber proves possession by disclosing the private key to the CA.
(D) The subscriber generates their own unique public-private key pair locally.

**May/June 2019**

**86.** Match the certificate system types in List I with their characteristic descriptions in List II.
List I: (System Types)
P. Central Authority
Q. Hierarchical Authority
R. Web of Trust
S. Root public key
List II: (Characteristics)
1. Anyone with a certificate may act as a CA by signing another certificate.
2. Signs certificates for all top level authorities in a bureaucratic structure.
3. All certificates are signed by a single entity, and its key is embedded in checking software.
4. Delegates the ability to sign certificates through a bureaucratic hierarchy.
(A) P-3, Q-4, R-1, S-2
(B) P-4, Q-1, R-3, S-2
(C) P-1, Q-2, R-4, S-3
(D) P-2, Q-3, R-1, S-4

NODIA

**Oct/Nov 2016**

**87.** Which of the following is not mentioned as one of the network-connected things in the Internet of Things (IoT) relying on PKI for identity authentication?
(A) ATMs and financial accounts
(B) Submarine sonars and deep space satellites
(C) Home surveillance equipment and smart meters
(D) Planes, trains and automobiles

**May/June 2007**

**88.** Given below are two statements: one is labelled as Assertion (A) and the other is labelled as Reason (R).
Assertion (A): In India, the CCA acts at the root

end-users.
Which of the above statement(s) is/are correct?
(A) (I) and (II)
(B) (II) and (III)
(C) (I) and (III)
(D) (I), (II), and (III)

**Oct/Nov 2013**

**115.** An IT expert assesses an enterprise's file encryption protocol using AES-256. The expert notes that while 128-bit encryption is considered logically unbreakable as of date, breakability is relative to available technology. How does the expert justify the security of AES-256 in theory?
(A) It relies on an intrinsically linked handwritten signature for verification.
(B) It operates as a stream cipher, bypassing common block-level vulnerabilities.
(C) It employs an identical passphrase that is heavily hashed for every user.
(D) The key combination is massive, rendering it practically uncrackable.

**May/June 2020**

**116.** Consider the following process sequence for Voters List Preparation by the State Election Commission:
1. Digitize field data along with the photo ID.
2. Digitally sign the data to assure correctness.
3. Use the Digital Signature Certificate to counter verify the digitized data of voters list and photo ID.

Which of the following represents the correct sequence of events?
(A) 1, 2, 3
(B) 2, 1, 3
(C) 3, 2, 1
(D) 1, 3, 2

**Oct/Nov 2009**

**117.** Evaluate the following statements regarding blockchain and cryptocurrencies:
I Uses asymmetric cryptography for identity management.
II Users have public keys that everyone can see.
III Private keys are kept secret.
IV Bitcoin uses a cryptographic algorithm to ensure only legitimate owners can spend the funds.
V Ethereum relies on symmetric cryptography for its core ledger authentication.
Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (IV)
(B) (II), (III), (IV), and (V)
(C) (I), (III), (IV), and (V)
(D) (I), (II), (IV), and (V)

**May/June 2006**

**118.** Match the e-Governance initiative in List I with its description in List II.
List I: (Initiative)
P. Aadhaar Data Encryption
Q. Income Tax e-filing
R. MCA
S. Voters List Preparation
List II: (Description)
1. Revised provisions under section 44AB of IT Act make E-Filing mandatory above a threshold.
2. Secures resident demographics and biometrics using PKI-2048 and AES-256.
3. Field data and photo ID are digitized and signed to assure correctness of data.
4. Secures transactions related to the Registrar of Companies.
(A) P-2, Q-1, R-4, S-3
(B) P-1, Q-2, R-3, S-4
(C) P-3, Q-4, R-1, S-2
(D) P-4, Q-3, R-2, S-1

**Oct/Nov 2017**

**119.** A bank's security team is designing a key management system. They acknowledge that randomness does not come easily to computers and that the data is not secret unless the key is secret. According to basic issues in secret key management, what happens the more a key is used?
(A) The easier it is to crack.
(B) It becomes exponentially harder to guess.
(C) It automatically increases its key length to resist brute force.
(D) It naturally converts into an asymmetric public key.

**May/June 2018**

**120.** Given below are two statements: one is labelled as Assertion (A) and the other is labelled as Reason (R).
Assertion (A): Symmetric algorithms are preferred where the number of users is more, despite asymmetric algorithms being faster.
Reason (R): Rijndael algorithms are highly

NODIA

suitable for hardware level security in communicating devices.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2019**

**121.** Consider the following statements regarding cryptographic security:

I Communication environments require the identification of security issues.
II Cryptography can reformat and transformation data making it safer on its trip between computers.
III Security of information in transit is achieved by using different encryption techniques and protocols.
IV Applications of public and private keys provide defined protocols and standards.
V Certifying authorities distribute keys to the participants of electronic communication.

Which of the above statement(s) is/are correct?

(A) (I), (II), (III), and (IV)
(B) (II), (III), (IV), and (V)
(C) (I), (III), and (IV), and (V)
(D) (I), (II), (III), (IV), and (V)

**May/June 2015**

**122.** A user claims damages against a CA due to misrepresentation, stating the CA issued a certificate containing false information. How might the CA's liability for such claims be managed?

(A) It may be entirely dismissed by the local Registration Authority.
(B) It falls exclusively under the jurisdiction of the root public key owner.
(C) It may be limited either by law or by contract.
(D) It triggers an immediate global revocation of all TLS/SSL certificates.

**Oct/Nov 2023**

**123.** An enterprise decides to shift from a centralized trust model to a web-of-trust system for its internal developer communications. Which operational change must the developers expect regarding how certificates are handled?

(A) Certificates will strictly be signed by a single, central embedded key.
(B) Signing ability will be rigidly delegated through a bureaucratic hierarchy.
(C) Individuals judge certificates based on personal knowledge of the signers.
(D) The Root CA must personally issue every internal certificate for the staff.

**May/June 2022**

**124.** During a digital certificate forgery test, software rejects a certificate. What specific cryptographic process does this forgery test consist of?

(A) Verifying the certificate's digital signature by using the authority's public key.
(B) Verifying the certificate's digital signature by using the subscriber's private key.
(C) Comparing the SHA-256 hash against a 40-bit RC4 stream cipher.
(D) Scanning the document for intrinsic handwritten associations.

**Oct/Nov 2020**

**125.** Match the security concepts in List I with their appropriate application or tool in List II.

List I: (Security Concepts)
P. Eavesdropping prevention
Q. Message Integrity check
R. Non-repudiation enforcement
S. Revocation status check

List II: (Application/Tool)
1. Hash Functions / Message Digests
2. Digital Signatures
3. Encryption
4. CRL

(A) P-3, Q-1, R-2, S-4
(B) P-1, Q-2, R-3, S-4
(C) P-4, Q-3, R-1, S-2
(D) P-2, Q-4, R-3, S-1

www.nodia.in

Downloaded from www.pdf.tube

# ANSWERS

1. (D) The sender and receiver encrypt and decrypt the message with the same key.
Symmetric encryption uses a single shared secret key for both the encryption of plaintext and the decryption of ciphertext. This mathematical process ensures that any party possessing the specific key can transform the data. Because only one key is involved, it is highly efficient for processing large volumes of data rapidly during digital communication and storage.

2. (A) (I) and (II)
Passphrases often lack significant randomness because they are designed for human memorization, making them more predictable than random keys. Cryptographic software bridges this gap by applying hashing or key initialization to convert these strings into robust keys. However, for maximum security, all possible keys must be equally probable to prevent attackers from guessing more likely or common candidates.

3. (C) Decryption key
Within the mathematical framework of encryption, retrieving the original plaintext from an encoded ciphertext requires a specific decryption key. This component reverses the transformation applied by the encryption algorithm. Without this precise value, the data remains illegible, as the security of the message depends on the secrecy and mathematical uniqueness of the key used during the recovery phase.

4. (A) (I), (II), and (IV)
3DES enhances security by applying the DES algorithm three times, while AES offers robust protection through various key sizes selected via open competition. RC4 is a stream cipher that becomes vulnerable when using short keys of 40 bits or less. Unlike these, IDEA is a block cipher rather than a stream cipher, which distinguishes its fundamental operational mechanism.

5. (B) By encrypting with the recipient's public key for decryption via their private key.
Asymmetric encryption ensures secure delivery by utilizing a public key for encryption and a corresponding private key for decryption. This framework allows anyone to encrypt a message for a specific recipient using their publicly available key. Only the intended recipient, who holds the unique private key, can mathematically reverse the process to read the original content of the message.

6. (B) IDEA
The International Data Encryption Algorithm serves as a highly efficient block cipher specifically designed for software implementation. It offers significant advantages over legacy DES by providing stronger resistance against differential cryptanalysis. These characteristics make it a suitable replacement for older systems that require robust security and high performance across various computing environments without the overhead of asymmetric models.

7. (B) Cryptography
Cryptography represents the specialized field of study focused on securing data through transformation and reformatting. By converting readable information into an unreadable state during transmission, it protects messages from unauthorized access. This science ensures that data remains safe while traveling between computers, providing essential pillars of security such as confidentiality and integrity within modern digital communication and network systems.

8. (B) AES (Rijndael) due to algorithm speed and lower complexity.
Bulk encryption of large transaction files requires an algorithm that balances high speed with strong security. AES, also known as Rijndael, is ideally suited for this task due to its efficiency in both software and hardware. Unlike asymmetric methods, which are computationally intensive, this symmetric block cipher processes massive

NODIA

owner of the private key, thus establishing the sender's identity.

**44.** (A) (I) and (II)
The verification process involves decrypting the digital signature to obtain the original message digest and then generating a new digest from the received document. If these two values match perfectly, it confirms the message has not been altered. However, if they are equal, the message is considered authentic and untampered, contradicting the statement that equality indicates tampering or alteration.

**45.** (C) Both (I) and (II)
In the context of Public Key Infrastructure, a client is the individual who owns the key pair and maintains the authority to create or change them. A subject, as defined by a Certification Authority, is an entity granted a license specifically to use the key pair. Both roles are fundamental to the operation of the system, defining ownership and usage rights.

**46.** (A) (I), (II), (III), and (IV)
Symmetric ciphers typically use key lengths ranging from 40 to 256 bits, with 3DES potentially reaching 168 bits. AES-256 is a standard recommendation for internet security protocols like SSL/TLS, and IDEA is known for its resistance to differential cryptanalysis. However, RC4 is a stream cipher, not a block cipher, making the fifth statement in the list technically inaccurate and incorrect.

**47.** (B) Because the public key belongs to the impostor and not the named sender.
Even if the mathematical process of decryption succeeds, the assurance of authenticity is worthless if the public key itself was not legitimately associated with the purported sender. An impostor can generate a valid key pair and falsely claim an identity. Success only proves the message was signed by the owner of the corresponding private key, which in this case is the impostor.

**48.** (B) It is encrypted with the sender's private key.
To create a digital signature, the sender first generates a message digest through a hash function and then encrypts that digest using their own private key. This encryption step secures the digest and links it uniquely to the sender. The resulting signature can be verified by anyone with the sender's public key, proving that the sender created the original communication.

**49.** (A) Non-repudiation
Non-repudiation is the cryptographic property that prevents a sender from denying the origin or contents of their message. In financial transactions, this ensures that a client cannot later claim they did not place an order. Because a digital signature is unique to the document and the signer's private key, it provides legally recognized proof of the transaction, protecting the other party involved.

**50.** (B) It confirms the message was not altered, verifying its overall integrity.
When the decrypted message digest and the newly generated digest are identical, it provides mathematical proof that the message content remains exactly as it was when the signature was created. This match verifies the integrity of the data, ensuring no changes occurred during transmission. It is the primary method used to detect any tampering or corruption of electronic messages and documents.

**51.** (D) Assign individual keys to the authorized recipients within the database.
A correct step in managing secret keys involves carefully assigning unique keys to authorized recipients within a secure database. This ensures that only designated individuals can access or decrypt specific information. Procedures must avoid insecure broadcasting or sharing private keys with authorities, as the goal is to maintain strict confidentiality and individual accountability within the cryptographic system to prevent unauthorized data access.

**52.** (C) 256-bit (32-byte) hash
The SHA-256 algorithm is a widely used cryptographic hash function that always produces a fixed output size of 256 bits, regardless of the size of the input data. This 32-byte hash serves as a unique digital fingerprint of the original message. Its fixed length and high collision resistance make it an essential tool for ensuring data integrity and creating digital signatures.

Click Here to Buy book on Amazon

routing speed. In scenarios where the objective is related to network performance rather than data protection, the size of the cryptographic key is effectively irrelevant to the goal.

**18.** (A) The sender encrypts the message using the recipient's private key.
Asymmetric encryption, also known as public key encryption, involves a pair of mathematically linked keys. The sender must use the recipient's public key to encrypt a message, ensuring only the recipient can decrypt it. Encrypting with a private key is used for creating digital signatures, not for securing the message contents for a recipient, as private keys are never shared.

**19.** (D) The private key must be kept secret by its owner, while the public key may be shared with anyone.
The core principle of asymmetric cryptography is the distinct management of the two keys. The private key must always remain under the exclusive control of the owner and never be shared. Conversely, the public key is intended for wide distribution. This allows any user to encrypt data or verify signatures while ensuring that only the authorized owner can perform decryption.

**20.** (A) Key length : Fixed key length
Asymmetric cryptosystems are characterized by the use of variable key lengths, such as 1024, 2048, or 4096 bits, depending on the required security level. This flexibility distinguishes them from many traditional symmetric block ciphers that often use specific fixed key sizes. The ability to increase key length allows these systems to remain secure against advancing computational capabilities and sophisticated brute-force attacks.

**21.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
RC4 is frequently deployed with 128-bit keys to provide robust security against unauthorized access. This practice is necessary because shorter key lengths, particularly those of 40 bits or less, have been proven vulnerable to brute-force cracking. By using a longer key, the number of possible combinations increases exponentially, making it computationally impractical for attackers to succeed in a reasonable timeframe.

**22.** (B) Key
A key is a sequence of characters or bits used in conjunction with a cryptographic algorithm to transform data. It serves as the essential mathematical component that allows for the encryption and decryption of messages. Access to the correct key is the only way for an individual to recover the original information, thereby ensuring confidentiality and restricted access to sensitive digital content.

**23.** (B) Only (II)
AES was selected as the modern standard to replace DES due to its superior security and processing efficiency. While symmetric systems like AES are faster for data encryption, asymmetric systems actually provide much better scalability for key distribution in large networks. Therefore, the claim that asymmetric scalability is lower is incorrect, whereas the statement regarding the replacement of DES is accurate.

NODIA

**24.** (D) Its most often cited problem today is its relatively short 56-bit key length.
The Data Encryption Standard has been largely superseded because its 56-bit key length no longer provides adequate security. Modern computing power can brute-force a key of this size in a very short time. Although it was once a robust global standard, the limited number of possible key combinations is its primary weakness, necessitating the move to more secure algorithms.

**25.** (B) P-1, Q-2, R-3, S-4
Symmetric cryptosystems provide confidentiality and integrity using a single shared key. Asymmetric cryptosystems expand this by offering authentication and non-repudiation through a public-private key pair assigned to an entity. Matching these attributes involves identifying that symmetric systems rely on shared secrets for basic security, while asymmetric frameworks utilize mathematically linked pairs to support a broader range of legal requirements.

**26.** (D) Cryptographic algorithm
A cryptographic algorithm is the specific mathematical function used to perform the processes of encryption and decryption. These algorithms define the set of rules for transforming plaintext into ciphertext and vice

amounts of data rapidly while maintaining a low complexity.

**9.** (B) Hashing
Hashing is the mathematical process used to transform a variable-length passphrase or string of characters into a fixed-length key. This transformation is essential for cryptographic programs to create usable keys from human-readable passwords. The resulting hash serves as a unique digital representation, ensuring that the input data produces a consistent and secure key suitable for various encryption algorithms.

**10.** (C) Diffie-Hellman
Symmetric encryption algorithms like Twofish, Serpent, and Kuznyechik utilize a single shared key for both locking and unlocking data. In contrast, Diffie-Hellman is a protocol specifically designed for secure key exchange over an insecure channel. It falls under the category of asymmetric or public-key cryptography because it involves mathematical properties that allow two parties to establish a secret.

**11.** (D) 112-bit key 3DES and 128-bit IDEA keys
Maintaining security in critical applications necessitates the use of robust key lengths that resist brute-force attacks. While shorter keys like 40-bit or 56-bit lengths are now considered insecure against modern computing power, 112-bit 3DES and 128-bit IDEA provide a significantly higher level of protection. These lengths ensure that the cryptographic strength is sufficient for protecting sensitive information.

**12.** (C) Stream ciphers work on plaintext one bit at a time, while block ciphers work on groups of bits.
Symmetric ciphers are divided into two main categories based on their operational granularity. Stream ciphers process the input data continuously, transforming each individual bit of plaintext into ciphertext. Conversely, block ciphers divide the plaintext into fixed-size segments or groups of bits, such as 64 or 128 bits, and apply the encryption transformation to each block as a single unit.

**13.** (A) It offers high scalability for many users, suited for small data like digital signatures.
While RSA is computationally slower than symmetric algorithms, its asymmetric nature provides exceptional scalability in large networks. It eliminates the need for secure out-of-band key distribution between every pair of users. This makes it highly useful for handling small but critical data segments, such as digital signatures, where verifying identity and ensuring non-repudiation are more important than speed.

**14.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Asymmetric encryption is significantly slower than symmetric encryption because it relies on complex mathematical operations involving large prime numbers. These algorithms require more computational power to process data, leading to longer execution times. This complexity is necessary to maintain security with public and private key pairs, explaining why they are generally less efficient for bulk data encryption tasks.

**15.** (D) It uses 128-bit blocks and efficient software and hardware implementations.
The Advanced Encryption Standard is characterized by its use of 128-bit data blocks and its remarkable efficiency across various platforms. Unlike older standards, it was designed to be fast in both hardware and software. It supports multiple key lengths and offers a high level of security, making it the global standard for protecting sensitive information in modern computer networks.

**16.** (A) Plaintext
In the field of cryptography, plaintext refers to the original, unencrypted information that is readable by humans or machines. It serves as the input for an encryption algorithm, which transforms it into ciphertext to hide its meaning. Understanding this terminology is fundamental for grasping how data is protected during transmission, as the goal is always to prevent unauthorized plaintext recovery.

**17.** (A) When the key is used exclusively to reduce the speed of network packet routing.
Cryptographic key length is a measure of security strength, designed to protect messages from unauthorized disclosure and brute-force attacks. However, increasing the length of a key does not inherently address operational network issues like

Downloaded from www.pdf.tube

**35.** (A) The program decrypts the digital signature using the sender's private key to extract MD-s.
During the verification of a digital signature, the recipient's program must use the sender's public key to decrypt the signature and extract the original message digest. Using the private key for decryption is incorrect because private keys are never shared and are only used by the sender for signing. The recipient then compares the extracted digest with a newly generated one.

**36.** (A) Preventing cryptographic services from being used by unauthorized entities.
The fundamental objective of secret key management is ensuring that only authorized individuals can access cryptographic services. Since the security of the system relies entirely on the confidentiality of these keys, protecting them prevents unauthorized parties from decrypting data or creating valid signatures. This protection is a critical requirement for maintaining the overall trustworthiness and functional integrity of any public-key infrastructure.

**37.** (A) It is an asymmetric encryption technique utilizing a public and private key framework.
128-bit encryption is primarily a symmetric encryption method, such as AES, where the same key is used for both encoding and decoding data. While it is considered logically unbreakable and highly secure in modern contexts, it does not inherently rely on the public and private key pairs that characterize asymmetric frameworks. This distinction is vital for understanding how different cryptographic algorithms operate.

**38.** (D) Obfuscation
Digital signatures are designed to meet specific legal and business requirements, including authenticity, integrity, and non-repudiation. These properties ensure that the sender is identified, the message remains unaltered, and the transaction cannot be denied. Obfuscation, which involves making code or data difficult to understand, is not a primary legal requirement or a standard goal of a digital signature system.

**39.** (D) The document has not been altered either in transmission or storage.
Integrity provides the essential assurance that a digital document has remained complete and unchanged from the moment it was signed. This requirement is verified by comparing the original message digest with a new digest generated upon receipt. If the values match, it proves that no modifications, whether accidental or intentional, occurred during the document's journey through various storage and transmission stages.

**40.** (D) The manager's private key
To generate a digital signature, the signer must use their own unique private key. This key is mathematically linked to their public key but remains secret and under their exclusive control. By applying this private key to a message digest, the signer creates a signature that anyone can then verify using the signer's corresponding public key, confirming the origin of the message.

**41.** (B) To deliver both the public key and the correct name of its owner safely.
The primary challenge in public key distribution is establishing a reliable link between the key and the identity of its owner. Without this verified association, an attacker could distribute their own public key under another person's name. Ensuring that the recipient receives the genuine public key alongside the correct, verified name of the owner is essential for the system's overall security.

**42.** (B) Only (II)
The SHA-256 algorithm is a modern cryptographic hash function that produces a unique, fixed-size 256-bit hash, providing a high level of security. Conversely, MD5 is considered unreliable for secure applications today due to its susceptibility to collision attacks, where different inputs produce the same hash. Therefore, while SHA-256 remains a robust standard, MD5 is no longer considered free from flaws.

**43.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Decrypting a digital signature allows the recipient to verify message authenticity because of the unique mathematical relationship between keys. In asymmetric cryptography, a signature created with a sender's private key can only be successfully decrypted using that sender's specific public key. This mechanism confirms that the signature must have originated from the

NODIA

**62.** (A) Repository
A repository functions as a centralized electronic database that stores and manages digital certificates. Similar to a public directory, it allows users to search for and retrieve the public keys of other entities. This facility is essential for the wide-scale implementation of public key infrastructure, providing a reliable location for accessing the credentials needed to verify digital signatures and encrypt messages.

**63.** (A) By checking it with the CA's public key.
To verify the signature on a digital certificate, a recipient must use the public key of the Certification Authority that issued it. Since the CA signed the certificate using its own private key, only the corresponding public key can successfully validate the signature. This verification confirms that the certificate was indeed issued by the trusted authority and has not been forged.

**64.** (C) The Registration Authority that encrypts the final message payload.
A typical digitally signed communication involves the sender, the recipient, and the Certification Authority. The sender signs the message, the recipient verifies it, and the CA issues the certificate that facilitates this trust. However, the Registration Authority primarily handles identity verification and does not perform the task of encrypting the final message payload, which is usually handled by the sender's software.

**65.** (A) The CA's public key
Cryptographic software must be configured with the public key of the trusted Certification Authority to verify the certificates it issues. This key is often hard-coded or securely loaded into the program during installation. By using the CA's public key, the software can automatically check the digital signatures on certificates, ensuring they are genuine and originated from the recognized issuing authority.

**66.** (A) (I) and (II)
The Internet of Things relies heavily on Public Key Infrastructure to provide a transparent and consistent method for certificate-based identity authentication. This is essential for securing the vast number of interconnected devices and applications in modern networks. While mobility and IoT introduce new challenges, the fundamental security requirements remain similar to earlier connected devices, focused on establishing trust and identity.

**67.** (D) (I), (II), and (III)
A standard public key certificate contains the name of the entity, its public key, and a digital signature created by a trusted authority. Together, these elements provide a verified link between an identity and a cryptographic key. The signature covers the other data in the certificate, ensuring that the information has not been altered and was indeed validated by the issuing authority.

**68.** (B) The subscriber generates his/her own public-private key pair.
In the certification process, the subscriber is responsible for generating their own unique pair of public and private keys. This step ensures that the private key remains under the subscriber's exclusive control from the moment of its creation. The public key is then submitted to the Certification Authority for validation and inclusion in a digital certificate, while the private key is never shared.

**69.** (A) A few multinational companies hold the market due to technical barriers.
The global market for trusted server certificates is dominated by a small number of multinational corporations. These companies possess the necessary technical infrastructure and established reputation to be recognized by major web browsers and operating systems. This concentration of authority is driven by the significant barriers to entry and the high level of trust required to operate as a globally recognized CA.

**70.** (C) Hierarchical Authority
A hierarchical authority system is designed for organizations that require multiple layers of certification, allowing for the delegation of signing authority through a structured bureaucracy. In this model, a root CA signs certificates for subordinate authorities, which in turn sign for others. This structure is ideal for large, complex systems where a single central authority would be impractical for managing all certificates.

Click Here to Buy book on Amazon

**53.** (C) Public keys are shared via online databases or trusted public repositories.
Digital signatures rely on the open distribution of public keys to enable verification of signed messages. These keys are typically stored in online databases or public repositories where they can be accessed by any recipient. Unlike private keys, which must remain secret, public keys are intended for general use, allowing the community to verify the authenticity and integrity of various digital communications.

**54.** (C) Public-private key pairs have an intrinsic association with a person similar to unique handwriting.
Unlike physical signatures, which are biologically linked to an individual through handwriting, public-private key pairs have no inherent, intrinsic connection to a specific person. They are merely mathematical values. Therefore, establishing a reliable association requires a trusted third party, such as a Certification Authority, to verify the owner's identity and bind it to the key pair through a digital certificate.

**55.** (A) P-2, Q-4, R-1, S-3
Authenticity confirms the source of a message, while integrity ensures that the document is accurate and complete. Non-repudiation holds the sender accountable for their communication, preventing denial of its origin. Verification is the specific technical process of checking if the extracted message digest matches the newly calculated one. Together, these requirements provide the legal and technical foundation for secure digital signatures.

**56.** (A) Message Digest
A message digest is the fixed-length sequence of bits produced by processing a message through a one-way hash function. This output serves as a unique representation of the original data. Because even a tiny change in the input results in a vastly different digest, it is an ideal tool for verifying that the content has not been altered since it was hashed.

**57.** (A) P-3, Q-4, R-1, S-2
Public Key Infrastructure provides the framework for distributing keys, while the client is the owner with rights to create them. A subject is the term used for a licensed user of a key pair. Digital certificates serve as the signed credentials within this system. Correctly identifying these roles is essential for managing trust and identity in a secure electronic environment or network.

**58.** (A) 2, 3, 1, 4
Creating a digital signature follows a specific chronological sequence. First, the message is processed through a hash function to generate a unique message digest. Next, this digest is encrypted using the sender's private key. Finally, the resulting encrypted signature is attached to the original message for transmission. This order ensures that the signature accurately represents the message and identifies the authorized sender.

**59.** (C) Authenticity
Authenticity is the security requirement focused on verifying the identity of the sender and the genuineness of the message. It answers critical questions about the source of the communication, ensuring that it originated from the purported sender and not an impostor. This property is vital in digital environments to establish trust and prevent fraudulent communications from being accepted as legitimate.

**60.** (C) Reject the message as it indicates the contents were tampered or altered.
If the extracted message digest does not match the newly generated one, the recipient must reject the message. This discrepancy is a clear indication that the content was modified, either accidentally or intentionally, after the signature was applied. Maintaining the integrity of the communication requires that only messages with perfectly matching digests be accepted as valid and trustworthy for processing.

**61.** (C) A root key or subordinate key received through manual distribution.
In a hierarchical certificate system, the validation process involves tracing a chain of signatures upward through multiple authorities. This chain eventually leads back to a trusted root key or a subordinate key that has been received through a reliable manual distribution method. By verifying each link in the chain, the user can ultimately establish trust in the original certificate's validity.

Downloaded from www.pdf.tube

versa. By utilizing these functions along with a key, users can protect sensitive information from unauthorized access, ensuring that the data remains secure during its transmission over various digital networks.

**27.** (B) 112 bits
3DES improves upon the security of the original Data Encryption Standard by applying the algorithm three times. When implemented using two independent keys, the effective total key length is 112 bits, as each DES key consists of 56 bits. This approach provides significantly higher resistance to brute-force attacks than a single 56-bit key, while remaining compatible with older legacy hardware and software.

**28.** (A) P-2, Q-1, R-3, S-4
RSA and Elliptic Curve Cryptography are examples of asymmetric encryption, as they utilize pairs of mathematically related public and private keys. In contrast, AES and Blowfish are symmetric encryption algorithms that rely on a single shared key for both the encryption and decryption processes. Correctly categorizing these algorithms is essential for understanding their specific roles in securing digital communications and data.

**29.** (D) Assertion (A) is false, but Reason (R) is true.
In cryptography, a key is a mathematical value derived from a passphrase but is not identical to it. While a passphrase is a human-readable string, a key is a specific sequence used by algorithms. However, the reason provided is correct because for a system to be secure against brute-force attacks, every possible key in the keyspace must have an equal probability.

**30.** (D) Key exchange : Out of band
Symmetric cryptosystems rely on a single shared key that must be kept secret between the sender and the receiver. Because the security of the entire system depends on this key remaining confidential, it must be exchanged through a secure, out-of-band channel. This ensures that an eavesdropper monitoring the main communication line cannot obtain the key and compromise the encrypted data.

**31.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Digital signatures differ from physical ones because they are mathematically tied to the content of the document. Any modification to the document, however slight, results in a completely different signature when the hash is recalculated. This unique document-signature relationship provides strong evidence of integrity, as the signature serves as a cryptographic verification that the specific file remains in its original state.

**32.** (A) (I), (II), and (IV)
Digital signatures provide authenticity by identifying the sender and integrity by ensuring the message is unaltered. To resolve disputes, parties must maintain records of all communications. However, non-repudiation actually prevents a sender from falsely claiming they did not send a message or that the content was different. Therefore, the statement suggesting non-repudiation allows such a claim is incorrect and misleading.

**33.** (B) In theory, it is not crackable since the combination of keys is massive.
AES-256 is considered theoretically unbreakable due to the enormous size of its keyspace. With 256 bits, the number of possible key combinations is so vast that even the most powerful supercomputers currently available would take billions of years to perform a successful brute-force attack. This massive mathematical complexity provides the high level of security required for modern internet communication protocols.

**34.** (D) Enlist a Certification Authority to link an entity with the key pair.
To ensure a public key belongs to the claimed individual, a trusted third party known as a Certification Authority is used. The CA verifies the identity of the entity and issues a digital certificate that mathematically binds the identity to the specific public key. This process prevents impostors from distributing bogus keys, providing a reliable basis for trust in public key infrastructures.

NODIA

71. (A) The private key
In the Bitcoin network, while public keys are visible to all participants, the private key must remain strictly secret. It is the only cryptographic element that allows a user to sign a transaction and prove ownership of their funds. Possessing the private key is equivalent to having the authority to spend the associated digital assets, making its protection the most critical security task.

72. (B) Random Distribution Authority
Trust models define the relationships between keys, certificates, and authorities. Common models include centralized authorities, hierarchical systems, and the global web of trust. However, a random distribution authority is not a recognized or used type of certificate system. Secure systems require structured methods for establishing trust to ensure that identities are correctly linked to public keys in a predictable manner.

73. (D) The subscriber's private key
A digital certificate is intended for public distribution and therefore never contains the subscriber's private key. Instead, it includes the public key, the subscriber's identity, an expiration date, and the digital signature of the issuing authority. The private key must always be kept secret by its owner to maintain the security and integrity of the entire asymmetric cryptographic system and its transactions.

74. (A) (I), (II), (III), and (V)
Public key certificates bind an identity to a key through a signature from a Certification Authority. Without checking this signature, an attacker could substitute a bogus key. Properly configured software uses the CA's public key—not the private key—to verify these certificates. This allows the system to automatically reject any certificates that were not issued by an authority it has been trained to recognize.

75. (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Public Key Infrastructure is essential for modern mobile environments because it provides a scalable way to secure diverse devices and applications. Mobile certificates are crucial for identifying authorized users and securing connections to corporate networks, cloud services, and payment systems. As mobile usage and BYOD policies grow, the need for a robust, certificate-based trust framework becomes increasingly critical for maintaining organizational security.

76. (D) It requires manual delivery because the public key's secrecy is critical.
Trusted manual distribution is used for root keys and other critical keys that form the basis of a trust chain. This method is required because the authenticity of the public key is paramount, not its secrecy. Public keys are designed to be shared openly; manual delivery simply ensures that the recipient receives the correct key from a verified source without any possibility of interception.

77. (D) A CA's liability for claims of negligence or misrepresentation may be limited either by law or by contract.
Certification Authorities hold a significant responsibility in maintaining the trust of a public key infrastructure. However, their liability in cases of negligence or incorrect information is not absolute. Legal frameworks and service contracts often include provisions that limit the financial or legal claims that can be made against a CA, balancing the need for accountability with the practicalities of providing certification services.

78. (A) (I), (II), and (III)
Centralized systems allow an authority to grant specific rights, while hierarchical models offer more flexibility through delegation. Web-of-trust systems rely on multiple signatures from various people rather than a single root key. In these decentralized models, individuals must make their own judgments about a certificate's validity based on their knowledge of the signers, rather than relying on a centralized root authority.

79. (C) Both (I) and (II)
Any objective third party with a strong reputation for credibility can function as a Certification Authority. To perform this role effectively, a CA may be supported by a Registration Authority, which handles the initial verification of a user's identity. This collaboration ensures that certificates are issued only to verified entities, maintaining the overall integrity and trustworthiness of the public key infrastructure.

Click Here to Buy book on Amazon

2. Replaces a failed drive while the server is still running
3. Drives share common disk controller circuitry
4. Each drive has its own controller circuitry

(A) P-3, Q-4, R-2, S-1
(B) P-4, Q-3, R-1, S-2
(C) P-2, Q-1, R-4, S-3
(D) P-1, Q-2, R-3, S-4

**Oct/Nov 2022**

**14.** What is the recommended timeframe within which trauma intervention should be initiated after an incident?
(A) 12 to 24 hours
(B) 24 to 48 hours
(C) 24 to 72 hours
(D) 48 to 96 hours

**May/June 2018**

**15.** Identify the correct statement regarding Phase 1 (Pre-Planning Activities) of the BCP Methodology.
(A) Focusing exclusively on the technical definition of short-term, intermediate-term, and long-term hardware outages.
(B) Executing the procurement and immediate installation of specialized recovery planning software for the entire bank.
(C) Initiating the actual execution of the formal plan testing and organizational exercising program for all departments.
(D) Developing interview schedules to conduct the security assessment and the detailed business impact analysis.

**Oct/Nov 2016**

**16.** How does the conceptual focus of a Disaster Recovery Plan (DRP) differ from that of a Business Continuity Plan (BCP)?
(A) BCP focuses on continuing key products and services, while DRP focuses on restoring technical infrastructure post-incident.
(B) DRP focuses on the tactical steps to maintain high-level business output, while BCP manages the technical hardware recovery.
(C) DRP primarily involves impact analysis and continuity strategy, while BCP is limited to initial damage assessment and site security.
(D) BCP is formulated after a disaster to manage recovery, whereas DRP is used as a preventive measure to avoid disasters.

NODIA

**May/June 2014**

**17.** What is the most appropriate reason for storing backup tapes in data safes?
(A) To shield magnetic media from environmental damage caused by fire, extreme heat, moisture, and air-borne particles.
(B) To ensure that LAN backup and restoration permissions are restricted exclusively to the senior systems administrator.
(C) To facilitate the generation of at least two redundant copies of all server backups for immediate on-site retrieval.
(D) To enforce the use of daily incremental backups as a method for reducing the volume of physical media required.

**Oct/Nov 2007**

**18.** All of the following are examples of business continuity risks EXCEPT:
(A) Normal employee attrition
(B) Cyberattacks and data breaches
(C) Unplanned IT and telecom outages
(D) Interruption to utility supply

**May/June 2025**

**19.** Consider the following statements regarding disk controller circuitry:
I In Disk Mirroring, a failure of the common disk controller puts access to either disk at risk.
II In Disk Duplexing, dual controllers can improve performance through a technique called split seeks.

Which of the given statements is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**Oct/Nov 2019**

**20.** Consider the following considerations in a trauma intervention plan:
I Ensuring trauma intervention is initiated within the first 24 to 72 hours.
II Making sure a good communication plan is in place.
III Providing lodging, food, and transportation for personnel.
IV Relying strictly on in-house expertise regardless of experience.

Which of the above statements are correct?

**89.** (A) P-2, Q-1, R-3, S-4
The CCA is appointed to sign CA public keys, while the RCAI is the root authority established under Indian law. The Registration Authority acts as the interface for user identity verification. Multinational companies like Symantec dominate the global market for server certificates. These entities perform distinct roles within the legal and technical infrastructure required for secure digital certification and internet communication.

**90.** (A) P-4, Q-2, R-3, S-1
Using an analogy of bank tellers, providing a CA's public key is like training tellers, and genuine certificates are like valid currency. Software rejecting bad certificates is like tellers rejecting forgeries. The forgery test itself is the verification of the digital signature using the authority's public key. This comparison helps illustrate the complex cryptographic processes involved in certificate validation and trust management.

**91.** (B) IRCTC : Facilitated online ticketing using DSCs for approved agents.
IRCTC has improved the security and efficiency of its online ticketing system by requiring approved agents to use Digital Signature Certificates. This ensures the authenticity of the agents and the integrity of the booking process. Such initiatives demonstrate the practical application of cryptographic tools in government services, providing a secure and legally recognized framework for conducting large-scale electronic commerce and public transactions.

**92.** (C) It is an asymmetric cipher primarily used to establish Web of Trust systems.
3DES is a symmetric block cipher that applies the Data Encryption Standard algorithm three times to data blocks. It is not an asymmetric cipher and is not used to establish web of trust systems, which rely on public-key pairs. Its primary purpose is to provide enhanced security for symmetric encryption by increasing the effective key length compared to the original single DES algorithm.

**93.** (C) It simplifies transactions with the Registrar of Companies and secures data.
Using a Digital Signature Certificate with the Ministry of Corporate Affairs streamlines various legal and administrative filings. It allows companies to interact with the Registrar of Companies electronically, ensuring that data is submitted securely and with verified authenticity. This modernization reduces the need for physical paperwork and provides a legally binding method for corporate houses to fulfill their statutory filing requirements.

**94.** (C) Attaches the CA's own digital signature to the certificate.
The subscriber is responsible for generating their key pair, providing proof of identity, and demonstrating possession of the private key. However, the final step of attaching the CA's digital signature to the certificate is performed exclusively by the Certification Authority. This signature is what validates the certificate and confirms that the CA has verified the link between the subscriber and their public key.

**95.** (B) Because a DSC ensures authenticity and is recognized under the legal system.
Documents uploaded to the DGFT website using a Digital Signature Certificate are legally equivalent to physically signed ones because the DSC provides strong proof of authenticity. The legal framework recognized by the IT Act ensures that these electronic signatures are valid for government and commercial transactions. This allows exporters and importers to conduct business online with the same legal certainty as traditional methods.

**96.** (B) It can deliver and manage many certificates at high speed transparently.
PKI is the ideal solution for large IoT networks, such as those used by utility companies for smart meters, because it can manage thousands of certificates efficiently. It provides an automated and transparent way to authenticate device identities and secure data transmissions across the network. This scalability and automation are essential for maintaining security in systems with a high volume of connected devices.

**97.** (D) (I), (II), (III), and (IV)
Aadhaar data security relies on a multi-layered approach using both asymmetric and symmetric encryption. Demographic and biometric data are encrypted at the point of collection using PKI-2048 and AES-256 standards. This combination is mathematically robust, and the time required

Downloaded from www.pdf.tube

**80.** (D) Because someone might substitute a bogus key or use a different name.
When submitting a public key to a CA, using a reliable delivery method is essential to prevent interception and tampering. An attacker could potentially replace the legitimate public key with a bogus one or associate the key with a different name. Ensuring the CA receives the exact key generated by the user is the first step in creating a trustworthy and valid digital certificate.

**81.** (C) Asymmetric cryptography
Blockchain technology uses asymmetric cryptography as its foundational security mechanism. Each user has a public key for identification and a private key for authorizing transactions through digital signatures. This framework allows for secure, peer-to-peer interactions without the need for a centralized authority, ensuring that only the rightful owner of a digital asset can spend it or transfer it to another party.

**82.** (A) The immediate local CA that signed the user's certificate.
In a hierarchical trust model, an individual validates a certificate by first checking the signature of the immediate local authority that issued it. This process continues upward through the chain of CAs until it reaches a trusted root. By verifying each link starting from the local level, the user can trace the legitimacy of the certificate back to a manually distributed, trusted key.

**83.** (D) IDRBT, NIC, TCS, NSDL, and CDAC are certifying authorities in India.
India has several established Certifying Authorities recognized under the Information Technology Act. These include organizations such as the National Informatics Center, Tata Consultancy Services, and the Institute of Development and Research in Banking Technology. These entities are authorized to issue digital signature certificates to various sectors, supporting the legal and technical requirements for secure electronic transactions across the country.

**84.** (C) Place the corresponding public key and its certificate on the CRL.
When a private key is compromised before its certificate expires, the CA must notify users that the key is no longer trustworthy. This is accomplished by adding the public key and its certificate to the Certificate Revocation List. Users and software checking the CRL will see that the key has been revoked and should no longer be used for verifying signatures or encrypting data.

**85.** (C) The subscriber proves possession by disclosing the private key to the CA.
A fundamental rule of asymmetric cryptography is that the private key must never be disclosed to anyone, including the Certification Authority. During the application process, a subscriber must prove they possess the private key, typically by signing a piece of data. They do not share the key itself. Instead, they provide proof of identity and their public key to obtain a valid certificate.

NODIA

**86.** (A) P-3, Q-4, R-1, S-2
Centralized systems use a single entity for signing all certificates, while hierarchical systems delegate this authority through a bureaucracy. In a web of trust, any certificate holder can act as a CA. Root public keys are those that sign for top-level authorities. These distinct characteristics define how trust is managed and distributed across different types of cryptographic networks and organizational structures.

**87.** (B) Submarine sonars and deep space satellites
While PKI is essential for securing a wide range of IoT devices, such as financial systems, home surveillance, and transportation networks, it is not specifically mentioned in the context of submarine sonars or deep space satellites. The focus of modern PKI adoption in IoT is primarily on terrestrial applications like smart meters and consumer electronics that require consistent identity authentication and secure connectivity.

**88.** (B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
The Controller of Certifying Authorities serves as the root of trust in India, certifying CA public keys. While it is true that the CCA was appointed under the IT Act, this appointment is a legal fact rather than a direct explanation of the CCA's technical role as the root of the trust chain. Both statements accurately reflect the legal and functional framework in India.

**106.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Income Tax regulations in India now mandate the use of Digital Signature Certificates for the e-filing of returns by certain professionals and individuals. Specifically, those with gross receipts exceeding fifty lakh rupees must comply with these revised provisions. This requirement ensures that high-value tax submissions are authenticated and protected, providing a secure and legally recognized method for electronic interaction with the tax authorities.

**107.** (A) The IT Act prohibits digital signatures for firms above 1 Crore turnover.
The Information Technology Act provides a legal framework for the use of digital signatures and the operation of Certifying Authorities in India. It does not prohibit their use based on a firm's turnover; rather, it encourages their adoption for secure electronic transactions. The appointment of the CCA and the establishment of the RCAI are key components of this system, supporting authentication for all entities.

**108.** (A) DGFT mandated DSC use with all electronic documents uploaded to their site.
The Directorate General of Foreign Trade has integrated Digital Signature Certificates into its electronic systems to enhance security and authenticity. By mandating the use of DSCs for all uploaded documents, the DGFT ensures that electronic submissions carry the same legal weight as traditional paper-based filings. This facilitates faster and more secure processing of licenses and other trade-related documentation for export and import organizations.

**109.** (A) P-3, Q-4, R-1, S-2
DES uses a 56-bit key, while 3DES with two keys has an effective length of 112 bits. IDEA is characterized by its 128-bit key block cipher design. RC4 becomes highly vulnerable to attacks when using key lengths of 40 bits or less. These varying key properties represent different eras and levels of cryptographic strength within the field of symmetric encryption and data protection.

**110.** (C) Public key encryption
Public key encryption is the most scalable choice for very large networks because it eliminates the complex problem of distributing a unique secret key to every possible pair of users. Instead, each user only needs their own key pair and access to a directory of others' public keys. This significantly reduces the administrative overhead and security risks associated with managing keys in massive user bases.

**111.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
The Certificate Revocation List is a critical component for maintaining trust when keys are lost or compromised. By placing a certificate on the CRL, the issuing authority informs all participants that the associated public key should no longer be trusted, even if it has not yet reached its scheduled expiration date. This immediate notification prevents the continued use of compromised keys, ensuring organizational security.

**112.** (B) Choice locking opted by the candidates.
In the process of online admission counselling, Digital Signature Certificates are used to perform the critical final step of choice locking. This ensures that the selections made by candidates are recorded accurately and cannot be altered after they are submitted. Using a DSC provides the necessary authenticity and integrity to finalize the choices, making the electronic process secure and reliable for both students and administrators.

**113.** (C) It will take billions of years to break the 2048-bit asymmetric encryption.
Breaking the 2048-bit asymmetric encryption used in Aadhaar data packets is computationally impossible with current technology. Even with millions of computers working together, the sheer number of possible key combinations is so vast that the process would take billions of years to complete. This mathematical robustness provides an extremely high level of protection for the demographics and biometrics stored within the enrolment packets.

**114.** (A) (I) and (II)
In India, several organizations like IDRBT, NIC, and TCS operate as Certifying Authorities, issuing certificates for various applications. While these entities handle end-user authentication, the Controller of Certifying Authorities functions

Click Here to Buy book on Amazon

at the root of the hierarchy to certify the CAs themselves. The CCA does not typically issue digital signature certificates directly to end-users, as that task is managed by the various licensed authorities.

**115.** (D) The key combination is massive, rendering it practically uncrackable.
The security of AES-256 is based on its massive keyspace, which contains an astronomical number of possible key combinations. This makes it practically impossible for an attacker to find the correct key through brute-force methods. While technological advancements always affect relative security, the sheer mathematical scale of a 256-bit key provides a level of protection that is expected to remain secure for the foreseeable future.

**116.** (A) 1, 2, 3
Preparing a voters list involves a clear sequence: digitizing field data and photos, digitally signing that data for correctness, and finally using the certificate to counter-verify the digitized information. This chronological order ensures that every piece of data is authenticated from the moment of entry. This systematic approach provides the necessary assurance of accuracy and integrity required for managing large-scale, sensitive election databases.

**117.** (A) (I), (II), (III), and (IV)
Blockchain and cryptocurrencies rely on asymmetric cryptography, where public keys identify users and secret private keys authorize spending. This framework is essential for managing digital identities and authenticating transactions. However, these systems do not rely on symmetric cryptography for their core ledger authentication, as that would require a shared secret which is incompatible with the decentralized nature of a public blockchain network.

**118.** (A) P-2, Q-1, R-4, S-3
Aadhaar uses advanced encryption for biometrics, while Income Tax regulations mandate e-filing for certain professionals. The Ministry of Corporate Affairs utilizes certificates for ROC transactions, and the election commission signs voter data to ensure correctness. Each of these initiatives leverages specific cryptographic tools to meet its unique security and administrative needs, demonstrating the versatility of PKI in modern government digital infrastructure.

NODIA

**119.** (A) The easier it is to crack.
A fundamental principle of secret key management is that the security of a key diminishes the more it is used. Extensive use of a single key provides an attacker with more encrypted data to analyze, which can reveal patterns and eventually make it easier to crack the code. To maintain high security, keys should be changed regularly to limit the amount of information protected by any one key.

**120.** (D) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
Symmetric algorithms are generally faster and highly efficient for hardware implementation. However, they are not preferred for large user bases due to the immense difficulty of securely distributing unique keys to every user pair. Asymmetric algorithms are used instead for their superior scalability in key management, even though they are slower. Both statements are factually correct but address different aspects of cryptographic systems.

**121.** (D) (I), (II), (III), (IV), and (V)
Cryptography provides a comprehensive set of tools and protocols for identifying security issues and protecting data in transit. By reformatting information and using both symmetric and asymmetric techniques, it ensures communication remains safe. The distribution of keys by Certifying Authorities is a vital part of this framework, providing the standards and trust necessary for secure electronic interaction across wide and diverse network environments.

**122.** (C) It may be limited either by law or by contract.
When a user claims damages against a Certification Authority due to misrepresentation or false information in a certificate, the CA's liability is not necessarily unlimited. Legal systems and service level agreements often provide specific limitations on the extent of the CA's financial and legal responsibility. This balanced approach allows CAs to operate while still being held accountable for their certification and identity verification processes.

**123.** (C) Individuals judge certificates based on personal knowledge of the signers.
In a web-of-trust system, the decentralized nature of the model means that there is no single root authority. Instead, users must rely on their own personal knowledge and trust in the individuals who have signed a certificate to judge its validity. This contrasts with centralized or hierarchical models where trust is established through a formal, bureaucratic chain leading back to a single, trusted central authority.

**124.** (A) Verifying the certificate's digital signature by using the authority's public key.
A forgery test in cryptographic software involves the specific process of validating the digital signature attached to a certificate. This is achieved by using the public key of the authority that purportedly issued it. If the signature is successfully verified, it proves the certificate is genuine and has not been altered, ensuring that the software only accepts valid credentials from recognized and trusted sources.

**125.** (A) P-3, Q-1, R-2, S-4
Cryptographic tools serve distinct security functions within a network. Encryption prevents eavesdropping by transforming data into an unreadable format. Hash functions or message digests are utilized for verifying message integrity. Digital signatures ensure non-repudiation by linking users to their communications. Finally, the certificate revocation list identifies keys that are no longer valid for use, completing the essential components of a secure framework.

www.nodia.in

NODIA

# CHAPTER 17

# Business Continuity & Disaster Recovery Planning

May/June 2016

**1.** Which combination of the following statements correctly identifies the objectives of a Business Continuity Plan (BCP)?

I Minimize financial loss to the institution.
II Continue to serve customers and financial market participants.
III Mitigate negative effects disruptions can have on reputation.
IV Ensure immediate evacuation of personnel post-disaster.
V Remain in compliance with applicable laws and regulations.

Which of the above statements are correct?
(A) Only (I), (II), (III), and (V)
(B) Only (II), (III), (IV), and (V)
(C) Only (I), (III), (IV), and (V)
(D) All (I), (II), (III), (IV), and (V)

Oct/Nov 2009

**2.** Conceptually, what happens in a mirrored disk failure scenario?
(A) The file server automatically deletes redundant data.
(B) The file server halts all operations until the damaged disk is replaced.
(C) The file server issues an alert and continues operating.
(D) The file server duplicates data across two entirely different physical locations.

May/June 2023

**3.** Which of the following elements is an exception and is NOT considered a part of a Disaster Recovery Plan (DRP)?
(A) Incident response
(B) Emergency response
(C) Business continuity strategy
(D) Evacuation plan

Oct/Nov 2018

**4.** Consider the following steps as part of the Miscellaneous Considerations for disaster management:

I Ensuring a water vacuum is available in case of flooding.
II Having a roll of plastic to cover equipment against sprinkler malfunction.
III Conducting regular inspections of the premises for safety measures.

Which of the given statements is/are correct?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) All (I), (II), and (III)

May/June 2007

**5.** Which of the following is a correct statement regarding Hardcopy Records?
(A) Off-site storage is unnecessary for most hardcopy records if they are shielded by waterproof containers and kept in-house.
(B) Fire resistant cabinets should be used to protect critical hard copy records from heat and smoke damage.
(C) Backup procedures for physical documents strictly exclude the use of high-capacity writeable CD-ROM or imaging technology.
(D) Hard copy records are considered immune to environmental water damage if they are stored inside standard industrial metal cabinets.

Oct/Nov 2025

**6.** What is the definition of the Vulnerability of a system?
(A) The total projected financial loss resulting from a sustained denial of access to critical system services and facilities.
(B) A weakness in internal controls, design, or implementation that could be exploited to cause a security breach.

Downloaded from www.pdf.tube

(C) The maximum duration a specific business unit can continue to operate without access to its primary information systems.
(D) A comprehensive inventory documenting all hardware, software, and communication equipment utilized by the organization.

**May/June 2012**

**7.** What is the definition of Business Continuity Planning (BCP)?
(A) A short-term tactical recovery plan designed to restore basic business functions immediately following a major catastrophic event.
(B) A strategic plan to ensure key products and services are delivered at predefined levels during a disaster.
(C) A collection of technical operational procedures developed for specific departments to restore critical software applications.
(D) A specialized emergency response protocol focused on the immediate evacuation of personnel and facility security measures.

**Oct/Nov 2014**

**8.** What is the definition of Hardware Redundancy in a LAN environment?
(A) A data management technique used to duplicate information from one primary hard disk to a secondary partition on that same disk.
(B) Provisions for maintaining continuous service by duplicating critical hardware components to mitigate system failures.
(C) A backup strategy that relies strictly on off-site tape rotations stored in climate-controlled data safes for disaster recovery.
(D) A security protocol that ensures administrative passwords are automatically rotated daily to prevent unauthorized system breaches.

**May/June 2019**

**9.** What is the minimum number of drives required to utilize the RAID 5 failure recovery mechanism?
(A) 2 drives
(B) 3 drives
(C) 4 drives
(D) 5 drives

**Oct/Nov 2006**

**10.** Identify the incorrect statement regarding Employee Awareness in a disaster avoidance program.
(A) Security and safety awareness is critical to any disaster avoidance program.
(B) Community service representatives should be excluded from speaking to employees to maintain internal confidentiality.
(C) Safety tips can be considered for insertion into pay-stub/cheque envelopes.
(D) Safety and security posters should be posted on Bulletin Boards throughout the organization.

**May/June 2021**

**11.** Which of the following is NOT an example of a vulnerability or exploit?
(A) An attacker uses an overflow weakness to install malware.
(B) An attacker convinces a user to open an email message with attached malware.
(C) A flood damages computer systems installed at the ground floor.
(D) A physical security guard actively intercepts unauthorized intruders at the server room door.

**Oct/Nov 2010**

**12.** Consider the following statements regarding planning divisions:
I BCP involves planning to continue business operations.
II DRP involves planning to recover from disaster situations.
Which of the given statements is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

NODIA

**May/June 2005**

**13.** Match the hardware redundancy techniques in List-I with their defining characteristics in List-II.
List I: Redundancy Techniques
P. Disk Mirroring
Q. Disk Duplexing
R. Disk Arrays
S. Hot Backup
List II: Characteristics
1. Two file servers operate in tandem

to break it through brute force using current technology is estimated to be billions of years, providing a high level of resident data protection.

**98.** (B) Only (II)
A message digest algorithm is a one-way hash function that transforms data into a fixed-length string that cannot be reversed. This property is fundamental for ensuring data integrity. While the second statement is correct, the first is inaccurate because the SHA-256 algorithm produces a 256-bit hash, not a 128-bit one. MD5 produces 128-bit hashes, but it is a different algorithm.

**99.** (B) Hierarchical systems : Anyone with a certificate acts exclusively as a single central authority.
In a hierarchical system, authority is delegated through a structured chain, where certain entities are authorized to sign certificates for others. It does not allow any certificate holder to act as a central authority. This differs from the web-of-trust model, where decentralized signing is common. Hierarchical models are designed to maintain a controlled, bureaucratic structure for managing trust across large organizations or systems.

**100.** (C) Remote work eliminates the need for Certificate Revocation Lists.
The transition to remote work has actually increased the visibility and importance of Public Key Infrastructure for securing digital trust and identity. While organizations are adopting zero-trust models and more advanced security measures, the need for Certificate Revocation Lists remains essential. CRLs are still required to identify and invalidate certificates that have been compromised or are no longer authorized for use in the network.

**101.** (B) (I), (II), and (IV)
Encryption is used to prevent eavesdropping, while non-repudiation ensures a sender cannot deny their communication. Digital signatures are a key tool for achieving non-repudiation in business. However, hashing alone cannot legally enforce non-repudiation because it does not identify the sender; it only proves that the data has not changed. Identification requires the use of a private key and a digital signature.

**102.** (A) Officials use digital signatures while vendors are limited to physical ones.
In India's e-Procurement systems, both government officials and vendors utilize digital signatures. This allows for a completely electronic tender process where all parties can authenticate their actions and ensure the integrity of their submissions. Vendors and traders are required to use Digital Signature Certificates to apply for tenders online, providing a secure and transparent environment for conducting public business and procurement.

**103.** (B) Its underlying mechanism resists differential cryptanalysis better than DES.
The International Data Encryption Algorithm provides superior security compared to DES due to its design, which is more resistant to differential cryptanalysis. It is a symmetric block cipher that is efficient to implement in software. These features made it a popular choice for various security applications during a period when the original DES algorithm was increasingly vulnerable to modern cryptographic attacks and computational power.

**104.** (D) (I), (II), (III), (IV), and (V)
PKI has proven to be a highly resilient technology over several decades, maintaining strong user confidence. It provides a practical and cost-effective method for addressing modern security challenges, such as identifying participants and securing messages. Through the distribution of keys by Certification Authorities, it enables a secure communication environment that meets the diverse needs of both individuals and large organizations in the digital age.

**105.** (C) Reducing AES block size to 56 bits for faster mobile packet routing.
The growth of mobile PKI is driven by the need to secure VPN connections, mobile payments, and BYOD environments. It provides a way to identify and authorize diverse mobile devices. However, reducing the AES block size to 56 bits is not a factor; in fact, reducing block size or key length would compromise security. AES maintains its 128-bit block size to ensure robust protection.

Click Here to Buy book on Amazon

(A) Only (I), (II), and (III)
(B) Only (II), (III), and (IV)
(C) Only (I), (III), and (IV)
(D) All (I), (II), (III), and (IV)

**May/June 2009**

**21.** Conceptually, what is the primary economic and business strategy perspective of Phase 2 (Vulnerability Assessment)?
(A) Implementing strategies that focus primarily on mitigating the financial impact of a disaster after it has happened.
(B) Ensuring that all vendor contract negotiations for tertiary recovery services are finalized before the next fiscal year.
(C) Prioritizing activities that reduce the likelihood of a disaster or security incident from occurring.
(D) Establishing a detailed profile of recovery resource requirements based strictly on short-term hardware outages.

**Oct/Nov 2011**

**22.** The following question consists of two statements, one labeled as Assertion (A) and the other as Reason (R). Examine these two statements carefully and select the correct answer.
Assertion (A): The Information Technology (IT) DRP is a typical example of a DRP developed for a specific group within an organization.
Reason (R): In the banking industry, BCP and DRP have a thin line of distinction because banking business operations and data processing operations are inseparable.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2010**

**23.** Which of the following is a correct statement regarding Fire Detection and Prevention?
(A) Business units have no role in ensuring fire suppression systems are adequate.
(B) Octopus wiring is recommended to minimize the number of required electrical outlets.
(C) Maintenance of exit signs is solely the responsibility of the local fire department.
(D) Exit signs should be checked regularly to ensure that they are lit.

**Oct/Nov 2024**

**24.** All of the following are recognized techniques to provide LAN hardware redundancy EXCEPT:
(A) Disk Mirroring
(B) Disk Duplexing
(C) Hot Backup
(D) Cold Site Replication

**May/June 2017**

**25.** Identify the incorrect statement regarding Local Area Network (LAN) backups.
(A) Provisions for scheduled, unattended backups of the server should be implemented.
(B) LAN backup and recovery functions should be accessible to all standard users.
(C) Backup of server files should happen on a nightly basis.
(D) At least two copies of the server backups should be generated.

**Oct/Nov 2005**

**26.** Match the planning activities in List-I with their corresponding plan type in List-II.
List I: Planning Activities
P. Impact analysis
Q. Damage assessment
R. Business continuity strategy
S. Emergency response
List II: Plan Type
1. DRP
2. BCP
3. BCP
4. DRP
(A) P-1, Q-4, R-2, S-3
(B) P-3, Q-2, R-4, S-1
(C) P-4, Q-3, R-1, S-2
(D) P-2, Q-1, R-3, S-4

**May/June 2020**

**27.** Match the BCP Phase numbers in List-I with their corresponding names in List-II.
List I: BCP Phase Number
P. Phase 1
Q. Phase 2
R. Phase 3
S. Phase 4

NODIA

List II: Phase Name
1. Detailed Definition of Requirements
2. Pre-Planning Activities
3. Vulnerability Assessment
4. Business Impact Assessment

(A) P-2, Q-3, R-4, S-1
(B) P-1, Q-4, R-2, S-3
(C) P-3, Q-1, R-4, S-2
(D) P-4, Q-2, R-1, S-3

**Oct/Nov 2015**

**28.** Consider the following steps included in the guidelines for Business Resumption/Continuity and Disaster Recovery plans:
I Fire detection and prevention
II Local area networks considerations
III Human factor personnel considerations
Which of the given statements is/are correct?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) All (I), (II), and (III)

**May/June 2013**

**29.** The following question consists of two statements, one labeled as Assertion (A) and the other as Reason (R). Examine these two statements carefully and select the correct answer.
Assertion (A): Disk Duplexing can improve performance by sending read requests to whichever disk can respond first.
Reason (R): Disk Duplexing utilizes a technique called "split seeks" enabled by dual controllers.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2021**

**30.** What is the most appropriate approach when dealing with the Human Factor during post-crisis response if in-house expertise is unavailable?
(A) Disregard the trauma intervention plan to preserve organizational financial resources and focus on technical recovery steps.
(B) Rely exclusively on standard internal human resources indoctrination programs and routine employee assistance policies.
(C) Postpone all intervention activities until the primary business software applications are confirmed to be fully operational.
(D) Hire external professionals with specialized experience in managing post-crisis psychological response and employee support.

**May/June 2024**

**31.** Consider the following statements regarding the sequential phases of BCP:
I Phase 3 develops a profile of recovery requirements based on short, intermediate, and long term outages.
II Phase 4 utilizes the BIA Report to identify critical systems and functions.
Which of the given statements is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**Oct/Nov 2008**

**32.** Which combination of factors must be considered while designing the BCP according to the RBI Guidelines?
I Probability of unplanned events including natural or man-made disasters.
II Security threats.
III Increasing infrastructure and application interdependencies.
IV Failure of key third party arrangements.
V Globalization and the challenges of operating in multiple countries.
Which of the above statements are correct?
(A) Only (I), (II), (III), and (IV)
(B) Only (II), (III), (IV), and (V)
(C) Only (I), (III), (IV), and (V)
(D) All (I), (II), (III), (IV), and (V)

**May/June 2006**

**33.** Identify the incorrect statement regarding the Business Impact Assessment (BIA).
(A) It is the most important task and can be called the heart of all BCP and DRP exercises.
(B) It assesses the length of time business units can survive without access to systems.
(C) It helps in setting the order of priority for systems to be restored/recovered.
(D) The BIA Report is presented exclusively to

Downloaded from www.pdf.tube

# STUDYING FROM PDFs?

# THINK AGAIN.

If you are studying only from PDFs,
you are wasting valuable time.

Research shows that learning from

**PRINTED BOOKS** has up to

**4× HIGHER RETENTION**

than studying from screens.

**PRINT BOOK = BETTER MEMORY**

**PDF = LOWER RETENTION**

Those who study from **PRINTED BOOKS**
move **AHEAD.**

Others are left **BEHIND**
in competition.

In competitive exams,
being average is not enough.

## STAY ONE STEP AHEAD.

the IT administration team.

Oct/Nov 2017

**34.** Which combination of incidents can prevent a bank from conducting business as usual, as listed under disaster avoidance?
I Extended power outages
II Equipment theft
III Chemical spills
Which of the above statements are correct?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) All (I), (II), and (III)

May/June 2008

**35.** Identify the correct statement regarding Phase 8 (Initial Plan Testing and Implementation).
(A) Phase 8 - Modifying the plans as appropriate based on test results.
(B) Phase 6 - Defining Recovery Teams, their roles and responsibilities.
(C) Phase 3 - Conducting the Security Assessment.
(D) Phase 1 - Evaluating alternative testing strategies.

Oct/Nov 2013

**36.** What is the definition of Disaster Recovery?
(A) The ability to restore business operations quickly following an event that disrupts information flow.
(B) The strategic negotiation of standby agreements with local equipment dealers prior to an emergency situation.
(C) The detailed process of assessing economic impacts to determine the survival threshold for each business unit.
(D) The physical replication of a secondary disk controller to enable simultaneous read requests and split seeks.

May/June 2015

**37.** Consider the following tasks included in Phase 2 (Vulnerability Assessment and General Definition of Requirements):
I A thorough Security Assessment of the computing environment.
II Presenting findings and recommendations to the Steering Committee.
III Defining the scope of the planning effort.
IV Developing a Plan Framework.
V Assembling Project Team and conducting awareness sessions.
Which of the above statements are correct?
(A) Only (I), (II), (III), and (IV)
(B) Only (II), (III), (IV), and (V)
(C) Only (I), (II), (IV), and (V)
(D) All (I), (II), (III), (IV), and (V)

Oct/Nov 2012

**38.** Under the RBI Guidelines on Business Continuity Planning, what is the mandated threshold for reporting frauds to the Audit Committee of the Board?
(A) Above 10 lakh
(B) Above 50 lakh
(C) Above 5 crore
(D) Above 1 crore

May/June 2011

**39.** All of the following are considered Key Factors to be considered for BCP according to RBI Guidelines EXCEPT:
(A) Probability of bio-chemical disasters.
(B) Regulatory and compliance requirements which are growing increasingly complex.
(C) Failure of key third party arrangements.
(D) Decreasing infrastructure and application interdependencies.

NODIA

Oct/Nov 2020

**40.** Match the BCP Phase numbers in List-I with their corresponding names in List-II.
List I: BCP Phase Number
P. Phase 5
Q. Phase 6
R. Phase 7
S. Phase 8
List II: Phase Name
1. Maintenance Program
2. Plan Development
3. Initial Plan Testing and Implementation
4. Testing/Exercising Program
(A) P-2, Q-4, R-1, S-3
(B) P-1, Q-2, R-3, S-4
(C) P-4, Q-3, R-2, S-1
(D) P-3, Q-1, R-4, S-2

May/June 2022

**41.** Consider the following steps which constitute a robust disaster prevention and recovery model for back-up data handling:
I Determining how much time is needed for

Oct/Nov 2010

**54.** All of the following represent basic types of computing disasters EXCEPT:
(A) Natural disasters such as earthquakes and floods.
(B) Accidents such as a devastating fire or an airplane crash.
(C) Routine, planned server maintenance downtime.
(D) Deliberate actions like a disgruntled employee trashing key data.

May/June 2005

**55.** Identify the incorrect statement regarding the Roles, Responsibilities, and Organizational Structure as per RBI Guidelines.
(A) A junior official must be designated as the Head of BCP activity or function.
(B) Indian banks follow the RBI guideline of reporting specific frauds to the Audit Committee.
(C) BCP Committee or Crisis Management Team should be present in each department.
(D) There needs to be adequate teams for various aspects of BCP at central office and controlling offices.

Oct/Nov 2022

**56.** What is the most critical outcome delivered by the Business Impact Assessment (BIA) regarding system recovery?
(A) Identifying critical business functions and the specific timeframes in which they must be fully restored.
(B) Upgrading and documenting all existing data processing operating procedures for the primary data center.
(C) Developing and documenting alternative testing strategies tailored to the organization's unique environment.
(D) Formulating and implementing comprehensive change management procedures for the information technology department.

May/June 2018

**57.** Which combination of the following details should be included in a detailed inventory of equipment for disaster avoidance?
I Model & Serial Number
II Alternate Vendor/Supplier
III Availability
IV The physical weight of the hardware
Which of the above statements are correct?
(A) Only (I), (II), and (III)
(B) Only (II), (III), and (IV)
(C) Only (I), (III), and (IV)
(D) All (I), (II), (III), and (IV)

Oct/Nov 2016

**58.** Identify the incorrect statement regarding Phase 7 (Maintenance Program).
(A) Change management procedures are completely irrelevant in Phase 7.
(B) Maintenance of the plans is critical to the success of an actual recovery.
(C) The plans must reflect changes to the environments that are supported by the plans.
(D) It is critical that existing change management processes are revised to take recovery plan maintenance into account.

May/June 2014

**59.** The following question consists of two statements, one labeled as Assertion (A) and the other as Reason (R). Examine these two statements carefully and select the correct answer.
Assertion (A): BCPs should be maintained by annual reviews and updates to ensure their continued effectiveness.
Reason (R): A copy of the BCP, approved by the Board, must be forwarded for perusal to the RBI on an annual basis.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Oct/Nov 2007

**60.** What is the most appropriate primary benefit of having an ISO 22301-compliant BCMS regarding corporate reputation?
(A) It ensures that the organization pays the minimum possible premium for cyber insurance.
(B) It increases customer confidence in the organization's ability to respond to incidents.
(C) It guarantees absolute immunity from all

Click Here to Buy book on Amazon

but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2007**

**47.** Identify the incorrect statement regarding Disaster Avoidance.
(A) It encompasses steps a bank can take that enable it to respond in stride to any events.
(B) It provides absolutely foolproof protection from all types of damage, including human malice.
(C) High availability, redundancy, and failover are mantras of this process.
(D) It is a very cost-effective activity that is often neglected.

**Oct/Nov 2025**

**48.** Consider the following activities occurring during Phase 5 (Plan Development):
I Defining recovery plan components and documenting plans.
II Upgrading existing data processing operating procedures.
III Negotiating vendor contracts with suppliers of recovery services.
IV Conducting initial tests of the plans and modifying them.
Which of the above statements are correct?
(A) Only (I), (II), and (III)
(B) Only (II), (III), and (IV)
(C) Only (I), (III), and (IV)
(D) All (I), (II), (III), and (IV)

**May/June 2012**

**49.** Identify the correct statement regarding the Testing of a BCP as per RBI Guidelines.
(A) Banks should consider having unplanned BCP drills.
(B) Testing of BCP should exclusively focus on technology resources.
(C) Banks should actively avoid unplanned BCP drills to prevent operational panic.
(D) Internal Auditors should be excluded from auditing the effectiveness of BCP.

**Oct/Nov 2014**

**50.** Consider the following benefits of an ISO 22301-compliant business continuity management system:
I Protecting assets, turnover, and profits.
II Ensuring business continuity and maintaining service levels.
III Assisting leaders in making quick decisions.
Which of the above statements are correct?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) All (I), (II), and (III)

**May/June 2019**

**51.** Identify the incorrect statement regarding Back-up Basics.
(A) Banks should store back-up copies strictly on-site to ensure immediate retrieval.
(B) A classic distributed back-up model can be implemented for robust data handling.
(C) Automatic tape verification should be used to confirm data was written.
(D) Back-up copies should be stored off-site in a safe, dry, dust-free place.

**Oct/Nov 2006**

**52.** Identify the correct statement regarding Phase 4 (Detailed Definition of Requirements).
(A) Focusing on the systematic upgrading of all existing data processing and operational procedures for the bank.
(B) Evaluating various alternative testing strategies to establish a permanent and on-going testing program.
(C) Performing a comprehensive security assessment of the organization's internal personnel and hiring practices.
(D) Developing a recovery profile identifying essential resources like hardware, software, and key personnel.

**May/June 2021**

**53.** Arrange the following specific activities of Phase 8 (Initial Plan Testing and Implementation) in the correct chronological order:
1. Structuring the test
2. Defining the test purpose/approach
3. Analysing test results
4. Conducting the test
(A) 2, 1, 4, 3
(B) 1, 2, 3, 4
(C) 2, 4, 1, 3
(D) 4, 3, 2, 1

Downloaded from www.pdf.tube

4. Continuous/Distributed model

(A) P-1, Q-2, R-3, S-4
(B) P-3, Q-1, R-2, S-4
(C) P-2, Q-4, R-3, S-1
(D) P-4, Q-3, R-1, S-2

**Oct/Nov 2005**

**68.** Identify the incorrect statement regarding DR plan Testing and Maintenance.

(A) Read Through Test involves distributing copies to members for review.
(B) Structured Walk Through Test is a live operational failover to a Hot Site.
(C) Parallel Test involves implementing site activation procedure from the DR site.
(D) DR plan must be tested at periodical intervals to ensure viability.

**May/June 2020**

**69.** Consider the following recognized benefits of an incident response plan:

I Streamlining forensic analysis.
II Hastening recovery time.
III Increasing negative publicity to draw legal support.
IV Increasing the confidence of corporate executives and shareholders.
V Outlining how to minimize the duration and damage from a security incident.

Which of the above statements are correct?

(A) Only (I), (II), IV), and (V)
(B) Only (II), (III), (IV), and (V)
(C) Only (I), (III), (IV), and (V)
(D) All (I), (II), (III), (IV), and (V)

**Oct/Nov 2015**

**70.** Match the Disaster Recovery Strategies in List-I with their characteristic features in List-II.

List I: DR Strategy

P. Cold Site Replication
Q. Warm Site Replication
R. Hot Site Replication
S. Mirrored Environment

List II: Characteristic Features

1. Hardware needs to be purchased or leased, recovery in hours
2. Hardware is optional, lowest cost solution
3. Fully redundant, almost immediate restoration
4. High end solution, recovery extending to 10 minutes

(A) P-1, Q-2, R-4, S-3
(B) P-3, Q-4, R-1, S-2
(C) P-2, Q-1, R-4, S-3
(D) P-4, Q-3, R-2, S-1

**May/June 2013**

**71.** The following question consists of two statements, one labeled as Assertion (A) and the other as Reason (R). Examine these two statements carefully and select the correct answer.

Assertion (A): Automation in incident response helps businesses achieve a reliable, round-the-clock available system.

Reason (R): The time lag involved in manual response necessitates human intervention for typical repetitive tasks.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2021**

**72.** The following question consists of two statements, one labeled as Assertion (A) and the other as Reason (R). Examine these two statements carefully and select the correct answer.

Assertion (A): Storing media at an off-site location reduces the likelihood that the same event will affect both on-site data and backup.

Reason (R): Placing a break in the stream by taking the backup physically off-line protects against network-transmitted viruses.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2024**

**73.** All of the following are phases of the SANS Incident Response Plan EXCEPT:

(A) Preparation
(B) Identification
(C) Orchestration

NODIA

internal data breaches.
(D) It automates the generation of hardcopy records for critical operations.

**May/June 2025**

**61.** What is the most appropriate strategy for protecting against an internal act of sabotage by an embezzler attempting to cover their trail?
(A) Hot Site Replication
(B) Disk Mirroring
(C) Putting data "out of reach" via multiple tape generations
(D) Disk Duplexing

**Oct/Nov 2019**

**62.** Arrange the following phases of an Incident Response Plan according to the SANS Institute in chronological order:
1. Containment
2. Identification
3. Eradication
4. Preparation

(A) 4, 2, 1, 3
(B) 2, 4, 3, 1
(C) 1, 2, 3, 4
(D) 4, 1, 2, 3

**May/June 2009**

**63.** Conceptually, what is the primary risk of maintaining a mirror image of production data in an off-site facility without placing a break in the stream?
(A) A destructive virus in production data will immediately replicate to the mirrored backup environment.
(B) The physical transportation of backup media to a remote location takes too much operational time.
(C) Cybercriminals cannot gain access to mirrored systems over a high-speed wide area network.
(D) The split seek mechanism significantly delays the performance of daily production transactions.

**Oct/Nov 2011**

**64.** Identify the correct statement regarding the Basel Committee's report "Risk Management for Electronic Banking".
(A) Incident response mechanisms are largely irrelevant when managing operational risk in a bank.
(B) Incident response teams should be required to act strictly without any authority in an emergency.
(C) Effective incident response is critical for minimizing operational, legal, and reputational risks.
(D) Banks should avoid collecting forensic evidence to preserve storage space on production servers.

**May/June 2010**

**65.** Identify the correct statement regarding Hot Site Replication.
(A) A fully redundant environment allowing for recovery and restoration within seconds or minutes.
(B) A recovery strategy that relies exclusively on the restoration of data from physical tapes.
(C) A system architecture where the installation of hardware components is strictly optional.
(D) A configuration that does not require the replication of data via communication lines.

**Oct/Nov 2024**

**66.** Conceptually, what is the primary advantage of testing IT DRP plans rather than relying on assumed theoretical success?
(A) It identifies weaknesses in the plan and validates the ability to recover specific business applications.
(B) It ensures strict fulfillment of all ISO 27002 forensic evidence and auditing requirements.
(C) It allows the organization to bypass the Business Impact Assessment phase of the BCP methodology.
(D) It provides a method for the automated generation of decryption keys for ransomware attacks.

**May/June 2017**

**67.** Match the back-up schedule types in List-I with their frequency in List-II.
List I: Back-up Schedule Types
P. Full back-ups
Q. Incremental back-ups
R. Selective back-ups
S. Local server back-up replication
List II: Frequency
1. Weekly
2. Daily
3. Monthly

Click Here to Buy book on Amazon

into the production environment

**Oct/Nov 2012**

**80.** Match the DR Testing Types in List-I with their descriptions in List-II.

List I: Testing Type

P. Read Through Test
Q. Structured Walk Through Test
R. Simulation Test
S. Parallel Test

List II: Description

1. A table top exercise involving role play against a scenario
2. Relocating personnel to alternate recovery site
3. Distributing copies of plans for review
4. Team members develop an appropriate response during a tabletop exercise

(A) P-1, Q-2, R-3, S-4
(B) P-3, Q-1, R-4, S-2
(C) P-4, Q-3, R-2, S-1
(D) P-2, Q-4, R-1, S-3

**May/June 2011**

**81.** What is the most appropriate reason why manual incident response is considered heavily flawed for cyber incidents?

(A) It requires the utilization of AI capability which manual responders cannot process.
(B) Manual response strictly violates the Basel Committee guidelines on paperless transactions.
(C) The time lag involved cannot guarantee an immediate response required for most cyber incidents.
(D) Human analysts are prohibited from updating firewall rules under ISO 27001.

**Oct/Nov 2020**

**82.** Consider the following statements regarding off-site and off-line data:

I Taking data off-site involves placing geographic distance between the data center and the vaulting site.
II Taking data off-line prevents a mirrored system from replicating a virus-infected file.

Which of the given statements is/are correct?

(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**May/June 2022**

**83.** What is the generally accepted recovery time for a Warm Site Replication strategy?

(A) Up to 10 minutes
(B) Up to 5 days
(C) Up to 10 days
(D) Up to 24 hours

**Oct/Nov 2023**

**84.** All of the following are examples of a security incident EXCEPT:

(A) Unauthorized computer or data access
(B) Physical or logical damage to systems
(C) Routine hardware redundancy disk mirroring
(D) Presence of a malicious application, such as a virus

**May/June 2016**

**85.** What is the definition of a Security Incident?

(A) A routine automated backup process that completes successfully outside of standard business hours.
(B) The organized archiving of physical records into a fire-resistant cabinet for long-term storage.
(C) An event that compromises or potentially compromises the operation of core systems or data assets.
(D) The structured review of an existing business impact analysis report by the management team.

**Oct/Nov 2009**

**86.** What is the typical recovery time for a Cold Site Replication strategy for a medium-sized bank?

(A) 1 to 8 hours
(B) 5 to 7 days
(C) 24 hours
(D) Less than 10 minutes

**May/June 2023**

**87.** Identify the incorrect pair regarding Disaster Recovery Strategies.

(A) Cold Site Replication - No Data Replicated via Communication Line
(B) Warm Site Replication - Medium Cost Solution
(C) Hot Site Replication - Lowest Cost Solution
(D) Hot Site Replication - Almost immediate Restoration

NODIA

(D) Lessons learned

**Oct/Nov 2008**

**74.** Identify the correctly matched pair regarding the Basel Committee's recommended functions for banks.

(A) Forensic evidence - Mechanisms to permanently delete compromised logs to limit liability.

(B) Crisis mechanism - Identify a crisis as soon as it occurs, assess materiality, and control reputation risk.

(C) Incident response teams - Personnel with no authority to act until the Board of Directors convenes.

(D) E-banking recovery - Plans restricted to non-geographic scenarios only.

**May/June 2006**

**75.** Consider the following functions highlighted by the Basel Committee that banks should develop for incident response:

I Mechanisms to assess the materiality of a crisis and control reputation risk.

II Incident response teams trained in interpreting the significance of related output.

III A process for collecting and preserving forensic evidence to assist in prosecution.

IV Ignoring post-mortem reviews to focus entirely on immediate future operations.

Which of the above statements are correct?

(A) Only (I), (II), and (III)

(B) Only (II), (III), and (IV)

(C) Only (I), (III), and (IV)

(D) All (I), (II), (III), and (IV)

**Oct/Nov 2017**

**76.** Consider the following statements describing factors to consider in tape drive performance and management:

I The 8-12 hour overnight back-up window may not be acceptable for the recovery window.

II Ultra-high capacity tape drives always represent high performance.

III Tape management software can place "mission-critical" data sets on high-performance class devices.

IV Archival data sets are best placed on ultra-high capacity helical scan or Digital Linear Tape devices.

Which of the above statements are correct?

(A) Only (I), (II), and (III)

(B) Only (II), (III), and (IV)

(C) Only (I), (III), and (IV)

(D) All (I), (II), (III), and (IV)

**May/June 2008**

**77.** Identify the incorrect statement regarding ISO 27001 and ISO 27002.

(A) ISO 27001 sets forth the compliance requirements needed to become certified.

(B) ISO 27002 provides detailed requirements for incident response and internal investigations.

(C) ISO 27002 helps introduce and implement information security best practices.

(D) ISO 27002 establishes strict mandatory certification protocols that supersede ISO 22301.

**Oct/Nov 2013**

**78.** The following question consists of two statements, one labeled as Assertion (A) and the other as Reason (R). Examine these two statements carefully and select the correct answer.

Assertion (A): In the event of internal sabotage, it is virtually impossible for the culprit to access and alter vaulted tape data without leaving evidence.

Reason (R): Vaulted tape data requires the embezzler or an accomplice to physically breach the vault and its security measures.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).

(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).

(C) Assertion (A) is true, but Reason (R) is false.

(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2015**

**79.** Identify the incorrect statement regarding the SANS Institute's incident response phases.

(A) Preparation - Preparing users and IT staff to handle potential incidents

(B) Containment - Finding the root cause of the incident and removing affected systems

(C) Identification - Determining whether an event is indeed a security incident

(D) Recovery - Permitting affected systems back

Downloaded from www.pdf.tube

the recovery.
II Implementing a classic distributed back-up model.
III Performing full back-ups daily instead of selectively.
IV Using automatic tape verification to confirm data was written.
V Storing the back-up copies off-site in a safe, dry, dust-free place.
Which of the above statements are correct?
(A) Only (I), (II), (III), and (IV)
(B) Only (I), (II), (IV), and (V)
(C) Only (II), (III), (IV), and (V)
(D) All (I), (II), (III), (IV), and (V)

**Oct/Nov 2023**

**42.** Conceptually, what does the term "pain threshold" refer to in the context of a Business Impact Assessment?
(A) The maximum financial expenditure a banking institution is willing to allocate for annual cyber insurance premiums.
(B) The total amount of physical impact or heat a server rack can withstand before experiencing a hardware failure.
(C) The maximum duration a business unit can operate without access to systems, services, and core facilities.
(D) The specific financial threshold set for negotiating emergency standby agreements with local equipment vendors.

**May/June 2016**

**43.** Match the Critical Components of Business Continuity Management in List-I with their descriptions in List-II as per RBI Guidelines.
List I: BCM Components
P. BCP Methodology
Q. Maintenance and Re-assessment
R. Procedural aspects
S. Infrastructural aspects
List II: Descriptions
1. Availability of basic amenities like electricity, water, and first-aid
2. Putting in place backup sites for critical payment systems
3. Utilizing inputs like ISO 22301
4. Annual reviews and updates to ensure continued effectiveness
(A) P-1, Q-2, R-3, S-4
(B) P-3, Q-4, R-2, S-1
(C) P-4, Q-3, R-1, S-2
(D) P-2, Q-1, R-4, S-3

**Oct/Nov 2009**

**44.** Identify the incorrect statement regarding ISO 22301.
(A) It sets out the requirements for a best-practice business continuity management system (BCMS).
(B) It provides businesses with up-to-date security and resilience certification.
(C) It enables organizations to protect their income stream in the aftermath of a disaster.
(D) It strictly prohibits the use of third-party evaluations of an organization's security posture.

NODIA

**May/June 2023**

**45.** The following question consists of two statements, one labeled as Assertion (A) and the other as Reason (R). Examine these two statements carefully and select the correct answer.
Assertion (A): Disaster avoidance provides foolproof protection from all types of damage.
Reason (R): High availability, redundancy, fault tolerance, and failover are key components of disaster avoidance.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2018**

**46.** The following question consists of two statements, one labeled as Assertion (A) and the other as Reason (R). Examine these two statements carefully and select the correct answer.
Assertion (A): Phase 2 of the BCP Methodology focuses on reducing the possibility of disaster occurrence.
Reason (R): From an economic perspective, it is preferable to concentrate primarily on minimizing the impact of an actual disaster.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true,

**Oct/Nov 2018**

**88.** What is the most appropriate reason for taking data "out of reach" by keeping multiple generations of data on tape at a remote location?

(A) To completely eliminate the logistical requirement for maintaining any on-site server backups.

(B) To provide protection against online attacks and viruses that mirrored systems cannot defend against.

(C) To ensure that disgruntled employees can quickly access and modify archived historical records.

(D) To minimize the geographic distance between the primary data center and the off-site vaulting facility.

**May/June 2007**

**89.** Conceptually, what distinguishes the Eradication phase from the Recovery phase in an incident response plan?

(A) Eradication focuses on limiting initial damage, while Recovery involves isolating all infected systems.

(B) Eradication removes the root cause, while Recovery safely returns systems to the production environment.

(C) Eradication focuses on preparing IT staff, while Recovery involves completing all incident documentation.

(D) Eradication identifies the security event, while Recovery involves finding the technical root cause.

**Oct/Nov 2025**

**90.** What is the primary reason for executing a Parallel Test during DR plan maintenance?

(A) To relocate personnel to the recovery site and perform duties as if an actual disaster occurred.

(B) To perform a basic tabletop role-playing exercise with the disaster recovery steering committee.

(C) To distribute copies of recovery plans to all team members for a non-actionable document review.

(D) To test the response of community service representatives and public relations teams exclusively.

**May/June 2012**

**91.** The following question consists of two statements, one labeled as Assertion (A) and the other as Reason (R). Examine these two statements carefully and select the correct answer.

Assertion (A): Most of the SOAR solutions available in the market today are offered with AI capability.

Reason (R): SOAR systems should translate standard security playbook operations to commands executed on the system.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).

(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).

(C) Assertion (A) is true, but Reason (R) is false.

(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2014**

**92.** Read the following scenario and answer the question that follows: Recognizing that the flood severely affected the morale and well-being of the staff, the BCP Head triggers the trauma intervention plan.

According to human factor guidelines, within what timeframe must this intervention ideally be initiated post-incident?

(A) 1 to 8 hours

(B) 8 to 12 hours

(C) 24 to 72 hours

(D) 5 to 7 days

**May/June 2019**

**93.** Consider the following statements regarding SOAR capabilities:

I Orchestration involves the coordination of actions across multiple security tools, IT systems, and human analysts.

II Automation strictly requires security analysts to write complex code to define workflows.

Which of the given statements is/are correct?

(A) Only (I)

(B) Only (II)

(C) Both (I) and (II)

(D) Neither (I) nor (II)

Click Here to Buy book on Amazon

**24.** (D) Cold Site Replication
Local area networks utilize several techniques to ensure hardware redundancy and high availability. Common methods include disk mirroring, disk duplexing, and hot backup servers that operate in tandem. These techniques provide immediate protection against component failure. Cold site replication, however, is a recovery strategy for an entire facility. It does not provide the immediate hardware-level redundancy required within a network.

**25.** (B) LAN backup and recovery functions should be accessible to all standard users.
Proper backup management for local area networks requires strict security controls. Access to backup and recovery functions must be limited to authorized administrative personnel to prevent unauthorized data access or tampering. Standard users should not have these permissions. Effective procedures include performing nightly backups, creating multiple copies, and implementing automated, unattended schedules to ensure consistent and reliable data protection.

**26.** (D) P-2, Q-1, R-3, S-4
Planning activities are categorized into either business continuity or disaster recovery. Business impact analysis and continuity strategy development are core components of business continuity planning. Conversely, damage assessment and emergency response protocols are tactical elements of disaster recovery planning. Understanding these distinctions helps organizations allocate resources correctly. This ensures both the maintenance of operations and technical restoration of systems.

**27.** (A) P-2, Q-3, R-4, S-1
The initial stages of the business continuity methodology follow a logical progression. Phase one involves pre-planning activities to organize the project. Phase two consists of a vulnerability assessment to identify risks. Phase three focuses on the business impact assessment to determine critical survival timeframes. Finally, phase four involves a detailed definition of requirements to specify the resources needed for recovery.

**28.** (D) All (I), (II), and (III)
Comprehensive guidelines for business resumption and disaster recovery cover multiple operational areas. Fire detection and prevention are essential for physical site security. Local area network considerations address the technical redundancy of data and hardware. Furthermore, human factor personnel considerations ensure that the well-being and support of staff are prioritized. These elements together form the basis of a functional framework.

NODIA

**29.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Disk duplexing enhances system performance by utilizing dual controllers to manage data requests. This configuration enables a technique known as split seeks, where read requests are sent to whichever disk can respond most quickly. Because each drive has its own dedicated path, the system can process multiple operations simultaneously. This architectural design directly results in faster data access and improved reliability.

**30.** (D) Hire external professionals with specialized experience in managing post-crisis psychological response and employee support.
Addressing the psychological impact of a crisis is a specialized task. If an organization lacks internal expertise in trauma management, it should hire external professionals with specific experience in post-crisis response. This approach ensures that employees receive the support needed to recover emotionally and professionally. Prioritizing human well-being is essential for long-term organizational stability and successful resumption of operations.

**31.** (D) Neither (I) nor (II)
In the standard business continuity methodology, phase three is the business impact assessment, which identifies critical systems. Phase four then uses that information to develop a detailed profile of recovery requirements based on various outage durations. The statements provided incorrectly attribute these tasks to the wrong phase numbers. Accurate phase mapping is necessary for a structured and effective planning process.

**32.** (D) All (I), (II), (III), and (IV) and (V)
According to RBI guidelines, designing a robust business continuity plan requires evaluating several complex factors. Banks must consider

(C) Ignoring
(D) Reducing

**May/June 2014**

**101.** Read the following scenario and answer the question that follows: Frustrated by the downtime, Gamma Bank's management considers paying the demanded ransom to regain access to their encrypted customer data.
Why do law enforcement and information security professionals advise against this action?
(A) Because it encourages cyber criminals to commit more attacks.
(B) Because paying a ransom automatically voids all cyber insurance policies globally.
(C) Because the bank's SOAR automation will block outgoing ransom payments.
(D) Because ISO 27001 imposes strict fines for negotiating with threat actors.

**Oct/Nov 2007**

**102.** All of the following represent examples where SOAR is applicable EXCEPT:
(A) An employee deliberately triggers a fire alarm as a prank without network interaction.
(B) Malware has infected systems.
(C) A system communicates with a Command & Control server via a RAT.
(D) Ransomware activity sets off an alarm in the middle of the night.

**May/June 2025**

**103.** Read the following scenario and answer the question that follows: During the activation of the secondary site, Alpha Bank's recovery team relocated completely to the alternate recovery site and implemented site activation procedures as if the disaster had just happened.
Which type of testing did they previously conduct to prepare for this specific physical relocation?
(A) Read Through Test
(B) Parallel Test
(C) Simulation Test
(D) Structured Walk Through Test

**Oct/Nov 2019**

**104.** What is the most appropriate reason an organization employs forensic cybersecurity professionals under their cyber insurance policy?
(A) To provide physical security for the personnel working at the cold site data center.
(B) To perform routine and mandatory employee security awareness training sessions.
(C) To negotiate equipment replacement costs and terms with local hardware vendors.
(D) To assist in determining what occurred during an attack and resolving the technical problem.

**May/June 2009**

**105.** Read the following scenario and answer the question that follows: The incident response team is mobilized. They locate the core server where the ransomware originated and physically remove the affected system from the production environment to eliminate the root cause.
According to the SANS Institute's phases, which phase is the team executing?
(A) Preparation
(B) Containment
(C) Eradication
(D) Recovery

**Oct/Nov 2011**

**106.** Match the automated incident response concepts in List-I with their examples in List-II.
List I: Concepts
P. Orchestration
Q. Automation
R. SOAR Integration
S. Proactive Response
List II: Examples
1. Triage alerts efficiently in real-time
2. Coordinating actions across multiple security tools and IT systems
3. Translating playbook operations to commands executed on the system
4. Using threat intelligence to detect malicious traffic automatically
(A) P-2, Q-3, R-4, S-1
(B) P-1, Q-2, R-3, S-4
(C) P-4, Q-1, R-2, S-3
(D) P-3, Q-4, R-1, S-2

NODIA

**May/June 2010**

**107.** Read the following scenario and answer the question that follows: To restore operations, Alpha Bank decides to activate a secondary site. The site they utilize requires hardware to be leased, synchronizes data periodically via a

**May/June 2015**

**121.** Read the following scenario and answer the question that follows: Following the audit, Delta Bank updates its BCP documents.
To comply with RBI requirements for the maintenance and re-assessment of plans, whose approval must the updated BCP receive before a copy is forwarded for perusal to the RBI on an annual basis?
(A) The LAN Administrator
(B) The Head of Human Resources
(C) The Lead Internal Auditor
(D) The Board

**Oct/Nov 2012**

**122.** Read the following scenario and answer the question that follows: Delta Bank is undergoing an annual audit of its BCP processes. During the review, the internal auditors uncover an internal financial fraud amounting to 1.5 crore.
According to RBI guidelines followed by Indian banks, to whom must this fraud be officially reported?
(A) The local community fire department
(B) The external SOAR vendor
(C) The Audit Committee of the Board
(D) The BCP Crisis Management Team exclusively

**May/June 2011**

**123.** Read the following scenario and answer the question that follows: To further demonstrate their operational resilience to regulators and gain a competitive advantage, Delta Bank's Steering Committee decides to pursue a formally recognized international certification for their entire Business Continuity Management System.
Which standard provides this certification?
(A) ISO 27001
(B) ISO 27002
(C) ISO 22301
(D) RAID 5 Certification

**Oct/Nov 2020**

**124.** Read the following scenario and answer the question that follows: The internal auditors also evaluate Delta Bank's BCP testing methodologies. They discover that the BCP team initiated a simulated disaster scenario without prior warning to the staff to test true readiness.
Is this action supported by RBI guidelines?
(A) Yes, RBI guidelines suggest that banks should consider having unplanned BCP drills.
(B) No, RBI mandates that all drills must be planned and notified 10 days in advance.
(C) No, unplanned drills strictly violate the Structured Walk Through Test protocol.
(D) Yes, but only if the test is a Parallel Test relocating all staff.

**May/June 2022**

**125.** Read the following scenario and answer the question that follows: Delta Bank operates a critical payment system that interacts directly with the data centers of the Reserve Bank. To ensure continuity, Delta Bank has established dedicated backup sites for these systems.
Under which critical component of BCM as per RBI guidelines does this action fall?
(A) BCP Methodology
(B) Procedural aspects of BCP
(C) Maintenance and Re-assessment of Plans
(D) Infrastructural aspects of BCP

www.nodia.in

Downloaded from www.pdf.tube

(A) Full backup
(B) Incremental backup
(C) Selective backup
(D) Mirrored backup

**May/June 2024**

**115.** Read the following scenario and answer the question that follows: Beta Bank's LAN administrator is upgrading the local server architecture to prevent outage during hardware failures. The administrator installs two hard disks operating in tandem, but ensures each drive has its own separate controller circuitry to enable read request optimization.
Which redundancy technique is being implemented?
(A) Disk Duplexing
(B) Disk Mirroring
(C) RAID 5 Arrays
(D) Hot Backup Servers

**Oct/Nov 2008**

**116.** Conceptually, what does orchestration in SOAR specifically enable during a virus detection event?
(A) It manually alerts the risk manager to evaluate the organization's need for additional insurance.
(B) It forces a mirrored disk to shut down its controller circuitry to prevent data from being written.
(C) It initiates a structured walk-through test for the disaster recovery team to perform a role play.
(D) It isolates threats by integrating with endpoint antivirus and automatically quarantining infected systems.

**May/June 2006**

**117.** Read the following scenario and answer the question that follows: Gamma Bank detects a ransomware attack at 2:00 AM. Their automated system detects the malicious IP via threat intelligence integration and immediately issues commands to the network firewalls to block the IP without human intervention.
Which specific capability of a SOAR system is demonstrated by translating standard security playbook operations to firewall commands?
(A) Identification
(B) Orchestration
(C) Simulation
(D) Automation

**Oct/Nov 2017**

**118.** Identify the correct statement regarding general cyber insurance coverage.
(A) It strictly refuses to cover any immediate financial costs associated with being a victim of an attack.
(B) It functions solely to replace physical computer equipment lost during severe natural disasters.
(C) It prohibits the employment of forensic cybersecurity professionals during an active investigation.
(D) It covers the immediate costs of a cyberattack, including data recovery and investigation expenses.

**May/June 2008**

**119.** Read the following scenario and answer the question that follows: Beta Bank decides to safely store the resulting backup tapes. To protect the magnetic media specifically from air-borne contaminants, heat, humidity, and magnetism, what is the required storage solution?
(A) Data safes designed for magnetic media
(B) Standard fire-resistant filing cabinets
(C) Ground floor storage lockers
(D) Octopus wired cabinets

**Oct/Nov 2013**

**120.** Match the ISO/Basel standards in List-I with their primary focus in List-II.
List I: Standards
P. ISO 22301
Q. ISO 27001
R. ISO 27002
S. Basel Committee Report
List II: Primary Focus
1. Guidelines for incident response and internal investigations
2. Risk Management for Electronic Banking
3. Compliance requirements needed to become certified in information security
4. Best-practice business continuity management system (BCMS)
(A) P-4, Q-3, R-1, S-2
(B) P-3, Q-4, R-2, S-1
(C) P-1, Q-2, R-3, S-4
(D) P-2, Q-1, R-4, S-3

NODIA

secure network, and promises a recovery time of 8 hours.
Which disaster recovery strategy has Alpha Bank employed?
(A) Cold Site Replication
(B) Hot Site Replication
(C) Local Area Network Array
(D) Warm Site Replication

**Oct/Nov 2024**

**108.** Conceptually, how is 'cyber insurance' utilized in the context of cyber risk management?
(A) It transfers residual cyber risk that cannot be addressed by avoiding, mitigating, or reducing.
(B) It acts as the primary and most effective method to completely avoid all types of cyber risk.
(C) It mitigates risk by automatically applying patches to software vulnerabilities across the network.
(D) It guarantees the immediate decryption of ransomware files without any third-party involvement.

**May/June 2017**

**109.** Read the following scenario and answer the question that follows: During the post-recovery briefing, the BCP Committee reviewed how well they met the "pain threshold" of the business.
In which specific phase of the BCP Methodology was this critical survival timeframe originally assessed?
(A) Phase 1 - Pre-Planning Activities
(B) Phase 2 - Vulnerability Assessment
(C) Phase 7 - Maintenance Program
(D) Phase 3 - Business Impact Assessment (BIA)

**Oct/Nov 2005**

**110.** Which combination of elements might be underwritten by cyber insurance according to standard procedures following a ransomware attack?
I Data recovery costs
II System forensics costs
III Costs of investigating what happened
Which of the above statements are correct?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) All (I), (II), and (III)

**May/June 2020**

**111.** Read the following scenario and answer the question that follows: Gamma Bank relies on an external policy provider to cover the substantial costs of hiring forensic cybersecurity professionals for the investigation.
What specific method of cyber risk treatment is Gamma Bank employing here?
(A) Risk avoidance
(B) Risk mitigation
(C) Risk reduction
(D) Risk transferring via cyber insurance

**Oct/Nov 2015**

**112.** Consider the following statements regarding the features of Automated Incident Response (SOAR):
I It addresses the difficulty of orchestrating people, processes, and technology manually.
II It expedites typical repetitive tasks with little or no human intervention.
III It refers to the proactive and systemic response to a security breach.
Which of the above statements are correct?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) All (I), (II), and (III)

**May/June 2013**

**113.** Identify the incorrect statement regarding the payment of ransoms in a cyberattack.
(A) Some cyber insurance companies cover the cost of actually giving in and paying a ransom.
(B) Paying a ransom is not recommended by the information security industry.
(C) Law enforcement strongly encourages paying ransoms to quickly recover operational capacity.
(D) Paying a ransom is discouraged because it encourages cyber criminals to commit more attacks.

**Oct/Nov 2021**

**114.** Read the following scenario and answer the question that follows: For daily operations, the administrator schedules backups where only the changed data sets are saved, prioritizing speed for medium recoveries.
According to back-up basics, what type of backup is this?

Click Here to Buy book on Amazon

# ANSWERS

1. (A) Only (I), (II), (III), and (V)
Business continuity focuses on maintaining operations and minimizing losses. Key objectives include serving customers and financial market participants without interruption. Plans aim to reduce financial losses and protect the institution's reputation during disruptions. Furthermore, staying compliant with legal and regulatory requirements remains a primary goal. While safety is vital, continuity emphasizes operational resilience and functional service delivery.

2. (C) The file server issues an alert and continues operating.
Disk mirroring involves maintaining two identical copies of data on separate hard drives. If one drive fails, the system provides redundancy by continuing to operate using the functional drive. The server typically issues an alert to notify administrators of the failure. This mechanism prevents data loss and ensures that business processes remain uninterrupted despite the hardware malfunction.

3. (C) Business continuity strategy
Disaster recovery specifically addresses the restoration of technical infrastructure and immediate emergency actions following an event. It encompasses incident response, evacuation protocols, and emergency response steps. Conversely, business continuity focuses on the strategic high-level plan to deliver products and services at predefined levels. Therefore, a strategic continuity approach is distinct from the tactical restoration focus of recovery plans.

4. (D) All (I), (II), and (III)
Comprehensive disaster management involves practical preventative measures for environmental hazards. Maintaining equipment like water vacuums prepares an organization for potential flooding scenarios. Using plastic rolls protects sensitive hardware from malfunctioning sprinkler systems. Regular inspections of the premises further enhance safety by identifying risks early. These activities collectively reduce the likelihood of avoidable physical damage to critical information systems.

5. (B) Fire resistant cabinets should be used to protect critical hard copy records from heat and smoke damage.
Protecting physical documents requires specialized storage solutions to withstand environmental threats. Fire-resistant cabinets are specifically designed to safeguard critical hardcopy records from damage caused by extreme heat and smoke during a fire. While digital backups are common, these physical containers provide an essential layer of security for original documents that must be preserved within the office.

6. (B) A weakness in internal controls, design, or implementation that could be exploited to cause a security breach.
In security contexts, vulnerability describes an inherent weakness or flaw within a system's internal controls, design, or implementation. Such weaknesses can be exploited by threats to cause a security breach or unauthorized access. Identifying these flaws is essential for risk assessment. Understanding vulnerabilities allows organizations to implement corrective measures and strengthen their overall security posture against potential exploits.

7. (B) A strategic plan to ensure key products and services are delivered at predefined levels during a disaster.
Business continuity planning represents a strategic approach for organizations to maintain essential operations during a crisis. It ensures that key products and services are delivered at predefined levels despite significant disruptions. Unlike short-term tactical recovery, it focuses on the resilience of the entire business process. This strategic planning helps minimize the negative impact on customers and financial stability.

NODIA

**Oct/Nov 2006**

**94.** Read the following scenario and answer the question that follows: The BCP Head instructs the LAN administrator to ensure that a highly destructive, self-replicating virus cannot instantly wipe out the backups along with the production data.
What is the most effective offline strategy prescribed to prevent this?
(A) Relying entirely on dual controllers to block the virus.
(B) Maintaining an active Hot Site Replication.
(C) Placing a break in the stream by taking the backup physically off-line.
(D) Replacing the failed drive while the server is still running.

**May/June 2021**

**95.** The following question consists of two statements, one labeled as Assertion (A) and the other as Reason (R). Examine these two statements carefully and select the correct answer.
Assertion (A): Law enforcement and the information security industry strongly encourage paying a ransom during a cyberattack.
Reason (R): Paying a ransom encourages cyber criminals to commit more attacks.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2010**

**96.** Read the following scenario and answer the question that follows: Gamma Bank decide to conduct an internal investigation to gather computer evidence for legal action.
To ensure the process is forensically sound and consistent with industry best practices, which ISO standard's guidelines should they strictly follow?
(A) ISO 22301
(B) ISO 27002
(C) ISO 27001
(D) Basel Committee Standard

**May/June 2005**

**97.** Identify the correct statement regarding Security Orchestration, Automation and Response (SOAR).
(A) SOAR relies primarily on the manual updating of firewalls to isolate various malicious IP addresses.
(B) SOAR functions are strictly limited to notifying human analysts without performing any automated actions.
(C) SOAR is primarily a hardware disaster avoidance tool designed to manage sudden hard drive crashes.
(D) Analysts should be able to define automated workflows without needing to be experts in writing code.

**Oct/Nov 2022**

**98.** Read the following scenario and answer the question that follows: Alpha Bank faces a severe flood that completely damages its ground-floor computer systems. Upon investigating the incident, the steering committee notes that the initial setup of servers on the ground floor was heavily flawed.
According to the BCP Methodology, what specific type of weakness does this represent?
(A) A vulnerability due to improper design and weakness in operations
(B) An exploitation of an overflow weakness
(C) A deliberate act of corporate espionage
(D) A failure in split seek duplication

**May/June 2018**

**99.** Read the following scenario and answer the question that follows: Beta Bank subsequently evaluates setting up a more advanced storage mechanism that allows replacing a failed drive without bringing the server down, requiring at least 3 drives.
What technology is under consideration?
(A) Disk Duplexing
(B) RAID 5 array
(C) Hot Backup
(D) Cold Site array

**Oct/Nov 2016**

**100.** All of the following are primary methods to address cyber risk before applying cyber insurance EXCEPT:
(A) Avoiding
(B) Mitigating

Downloaded from www.pdf.tube

16. (A) BCP focuses on continuing key products and services, while DRP focuses on restoring technical infrastructure post-incident.
Business continuity and disaster recovery serve distinct but complementary roles within an organization. Continuity planning is strategically focused on maintaining the delivery of key products and services during a crisis. In contrast, disaster recovery planning is more tactical, focusing on the restoration of the technical infrastructure and data systems. Together, they ensure the organization survives and recovers from major incidents.

17. (A) To shield magnetic media from environmental damage caused by fire, extreme heat, moisture, and air-borne particles.
Storing magnetic media requires specialized protection against various environmental threats. Data safes are used to shield backup tapes from extreme heat, moisture, and air-borne particles that could occur during a fire or disaster. This physical security ensures that the data remains readable and intact for recovery. Proper storage is a fundamental requirement for maintaining reliable and accessible backups.

18. (A) Normal employee attrition
Business continuity risks involve events that cause sudden and significant disruptions to normal operations. Common risks include cyberattacks, unplanned IT outages, and failures in utility supplies like electricity. While losing employees through normal attrition is a management challenge, it is generally considered a routine human resources issue. It does not typically constitute an emergency disruption managed under continuity plans.

19. (C) Both (I) and (II)
Disk mirroring utilizes a single controller, meaning a failure in that circuitry puts access to both mirrored disks at risk. Disk duplexing addresses this vulnerability by using dual controllers, providing a more robust redundancy solution. Furthermore, duplexing can improve system performance through split seeks. This technique allows the dual controllers to handle multiple read requests simultaneously, enhancing data access.

20. (A) Only (I), (II), and (III)
A robust trauma intervention plan prioritizes employee well-being after a major incident. It involves initiating support within seventy-two hours and maintaining a clear communication strategy. Practical support, such as providing food, lodging, and transportation, is also essential for staff. Organizations should avoid relying solely on inexperienced in-house staff and instead hire external professionals with specialized crisis management experience.

21. (C) Prioritizing activities that reduce the likelihood of a disaster or security incident from occurring.
The vulnerability assessment phase in business continuity methodology takes a proactive approach. It prioritizes activities and controls that reduce the likelihood of a disaster or security incident occurring. By identifying and mitigating weaknesses early, organizations can prevent costly disruptions. This preventive strategy is more cost-effective than focusing solely on reactive measures after a catastrophe has already taken place.

22. (B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
Information technology recovery plans are specific examples of disaster recovery plans developed for distinct organizational groups. In the banking sector, the distinction between business continuity and disaster recovery is often blurred because business operations depend heavily on data processing. While both statements are factual, the inherent link between banking data and operations does not explain why the IT plan is a subgroup.

23. (D) Exit signs should be checked regularly to ensure that they are lit.
Maintaining a safe environment requires regular checks of fire safety equipment. Exit signs must be inspected frequently to ensure they are lit and clearly visible to employees. While local authorities have a role, the organization itself is responsible for on-site safety measures. Proactive steps, such as avoiding octopus wiring, help prevent electrical fires and ensure that personnel are protected.

NODIA

**8.** (B) Provisions for maintaining continuous service by duplicating critical hardware components to mitigate system failures.
Hardware redundancy involves the duplication of critical system components to ensure continuous service in the event of a failure. By having backup hardware ready, organizations can mitigate the risk of system downtime. This technique is commonly applied to servers, power supplies, and network paths. It provides a robust foundation for high availability within a local area network environment.

**9.** (B) 3 drives
RAID level 5 utilizes block-level striping with distributed parity across the disks. To achieve this configuration and provide fault tolerance, a minimum of three physical drives is required. This setup allows the system to reconstruct data if a single drive fails. It offers a balanced approach between storage capacity, system performance, and data protection for organizational servers.

**10.** (B) Community service representatives should be excluded from speaking to employees to maintain internal confidentiality.
Effective disaster avoidance programs rely heavily on employee education regarding security and safety. Organizations should utilize various communication channels, such as posters and pay-stub inserts, to inform staff. Engaging external experts, including community service representatives, is encouraged to provide specialized knowledge. Excluding these experts would hinder the depth of safety training, as external perspectives often enhance internal preparedness.

**11.** (D) A physical security guard actively intercepts unauthorized intruders at the server room door.
Security incidents usually involve weaknesses like software overflows or physical vulnerabilities like ground-floor placement during floods. Social engineering that leads to malware installation is another common exploit. In contrast, a security guard actively stopping intruders is a functional control and a preventive measure. This action represents a successful security defense rather than a vulnerability that could be exploited.

**12.** (C) Both (I) and (II)
Organizations utilize different planning divisions to handle various aspects of crisis management. Business continuity planning involves strategies to keep essential business operations running during a disruption. Disaster recovery planning focuses specifically on the tactical steps needed to recover and restore systems after an incident occurs. Both disciplines are vital components of a comprehensive organizational resilience and risk management framework.

**13.** (A) P-3, Q-4, R-2, S-1
Hardware redundancy techniques vary by their architectural implementation. Disk mirroring involves two drives sharing common controller circuitry, whereas disk duplexing provides separate controllers for each drive to enhance reliability. Disk arrays allow for replacing failed drives while the server continues running. Finally, hot backup involves two file servers operating in tandem to provide immediate failover capabilities if needed.

**14.** (C) 24 to 72 hours
Managing the human factor after a crisis is a critical part of a recovery plan. Trauma intervention should be initiated quickly to support affected personnel and maintain morale. The recommended timeframe for beginning these support activities is between twenty-four and seventy-two hours following the incident. Timely response helps mitigate long-term psychological impacts and assists employees in returning to duties.

**15.** (D) Developing interview schedules to conduct the security assessment and the detailed business impact analysis.
The initial phase of business continuity methodology focuses on preparatory tasks to set the stage for detailed analysis. During this pre-planning stage, the project team develops interview schedules required for the security assessment and business impact analysis. These activities ensure that the planning effort is well-organized. It establishes the necessary groundwork before moving into strategic and technical assessment phases.

Click Here to Buy book on Amazon

the probability of natural or man-made disasters and various security threats. Infrastructure interdependencies and the potential failure of third-party arrangements also present significant risks. Additionally, globalization and the challenges of operating across multiple jurisdictions must be integrated into the organization's resilience strategy.

**33.** (D) The BIA Report is presented exclusively to the IT administration team.
The business impact assessment is the foundational element of continuity planning. It determines how long business units can survive without access to critical systems and helps prioritize recovery efforts. Because it addresses business survival, the final report must be presented to senior management and the steering committee. Ensuring high-level visibility allows for informed decision-making regarding organizational recovery priorities.

**34.** (D) All (I), (II), and (III)
Various incidents can disrupt a bank's ability to conduct normal business operations. Extended power outages stop electronic processing and communications. Equipment theft results in the loss of critical hardware and sensitive data. Chemical spills can make facilities inaccessible and hazardous to personnel. Recognizing these diverse threats is essential for disaster avoidance. Organizations must plan for technical failures and environmental events.

**35.** (A) Phase 8 - Modifying the plans as appropriate based on test results.
The business continuity methodology follows a specific sequence of activities. Phase eight involves initial plan testing and implementation, which includes modifying plans based on results. Other phases have different focuses; for instance, phase six involves plan development, and phase three is the impact assessment. Correctly identifying the tasks associated with each phase ensures a systematic and professional planning approach.

**36.** (A) The ability to restore business operations quickly following an event that disrupts information flow.
Disaster recovery is defined as the capability of an organization to quickly restore its business operations following an event that disrupts information flow. It focuses on the tactical restoration of technical systems, data, and communications. This process is essential for minimizing the downtime associated with catastrophic incidents. Effective recovery ensures that the organization resumes normal functions with minimal delay.

**37.** (D) All (I), (II), (III), (IV), and (V)
Phase two of the planning methodology involves a thorough vulnerability assessment and the definition of general requirements. Key tasks include conducting a security assessment, defining the project scope, and developing a plan framework. The project team is assembled, and awareness sessions are conducted to engage the organization. Finally, findings are presented to the steering committee to ensure support.

**38.** (D) Above 1 crore
Regulatory guidelines in India mandate strict reporting requirements for financial institutions. For frauds exceeding the threshold of one crore, banks are required to report the details directly to the Audit Committee of the Board. This ensures high-level oversight and transparency regarding significant financial losses. Proper reporting is a critical component of a bank's corporate governance and overall risk management framework.

**39.** (D) Decreasing infrastructure and application interdependencies.
Modern business continuity planning must account for several evolving risks. RBI guidelines highlight factors such as the probability of biochemical disasters and the increasing complexity of regulatory requirements. The failure of key third-party service providers is another significant concern. However, infrastructure and application interdependencies are actually increasing. This rising complexity makes the planning process more critical for stable banking operations.

**40.** (A) P-2, Q-4, R-1, S-3
The latter stages of the business continuity methodology focus on documentation and long-term viability. Phase five involves the actual development of the plan. Phase six establishes the testing and exercising program. Phase

Downloaded from www.pdf.tube

**90.** (A) To relocate personnel to the recovery site and perform duties as if an actual disaster occurred.
A parallel test is one of the most comprehensive ways to validate a disaster recovery plan. It involves the physical relocation of personnel to an alternate recovery site where they perform their actual job duties as if a disaster had occurred. This test checks technical systems and logistical elements. It ensures the organization can function from the secondary location during a crisis.

**91.** (B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
Most modern Security Orchestration, Automation, and Response (SOAR) solutions incorporate artificial intelligence to enhance their capabilities. These systems are designed to translate security playbooks into automated commands that the system can execute. While both statements describe important aspects of SOAR technology, the translation of playbooks into commands is a functional feature and does not explain why AI was adopted.

**92.** (C) 24 to 72 hours
Human factor guidelines emphasize that supporting the well-being of staff after a disaster is crucial for recovery. In scenarios where employees have faced significant stress, intervention must be initiated within a specific window to be most effective. The ideal timeframe for starting this support is between twenty-four and seventy-two hours after the incident. This timely response helps employees process the event.

**93.** (A) Only (I)
Orchestration in a SOAR system refers to the complex coordination of actions across various security tools, IT systems, and human experts. This integration streamlines the response to threats. Automation, on the other hand, is designed to simplify tasks; it should allow security analysts to define and execute workflows without needing to write complex code. Therefore, the first statement is correct while the second is not.

**94.** (C) Placing a break in the stream by taking the backup physically off-line.
To prevent a self-replicating virus from destroying backups along with production data, a physical break must be introduced. Real-time replication methods like mirroring or hot sites will copy the virus to the backup location instantly. By taking the backup physically off-line, the organization ensures that stored data is inaccessible to the network. This provides a safe, uninfected version for restoration.

**95.** (D) Assertion (A) is false, but Reason (R) is true.
Law enforcement and the information security industry strongly advise against paying ransoms during cyberattacks. Paying a ransom does not guarantee the return of data and encourages criminals to continue their activities and target more victims. Therefore, the assertion that paying is encouraged is false. Organizations are instead urged to rely on robust backup systems and incident response plans to recover operations.

**96.** (B) ISO 27002
When an organization needs to conduct a forensically sound internal investigation to gather evidence for legal action, specific standards provide the necessary guidance. ISO 27002 is the internationally recognized standard that offers detailed requirements and best practices for incident response and investigations. Following these guidelines ensures that evidence is handled correctly and remains admissible in court, supporting organizational legal objectives.

**97.** (D) Analysts should be able to define automated workflows without needing to be experts in writing code.
Security Orchestration, Automation, and Response (SOAR) is designed to enhance the efficiency of security teams. A key feature of modern SOAR solutions is that they should allow analysts to define and manage automated workflows without needing to write code. This capability enables faster response times and better coordination between tools. It moves beyond manual intervention to provide a systemic response.

NODIA

**49.** (A) Banks should consider having unplanned BCP drills.
According to RBI guidelines, testing the business continuity plan is essential for ensuring operational readiness. Banks are encouraged to conduct unplanned BCP drills to simulate real-world conditions and test the true responsiveness of their teams. Testing should not be limited to technology but must also include people and processes. Furthermore, internal auditors play a key role in auditing these plans.

**50.** (D) All (I), (II), and (III)
Implementing an ISO 22301-compliant system provides several strategic advantages for an organization. It helps protect critical assets, turnover, and profits by ensuring business continuity during disruptions. The standard also assists leaders in making quick, informed decisions during a crisis. By maintaining predefined service levels, the organization can preserve its reputation and customer confidence even when facing significant operational challenges or events.

**51.** (A) Banks should store back-up copies strictly on-site to ensure immediate retrieval.
Reliability in data protection requires that backup copies be stored off-site. Storing backups strictly on-site is dangerous because a single disaster could destroy both the original data and the backups. Proper procedures involve using a distributed backup model and automatic tape verification. Storing copies in a remote, safe environment ensures that data is available for restoration if the primary site fails.</ESTEM>

**52.** (D) Developing a recovery profile identifying essential resources like hardware, software, and key personnel.
Phase four of the methodology is dedicated to the detailed definition of requirements. During this stage, the organization develops a recovery profile that identifies the essential resources needed to maintain operations. This includes specifying required hardware, software, and key personnel. This detailed inventory ensures that the recovery plan is based on accurate resource needs, allowing for a more coordinated response.

**53.** (A) 2, 1, 4, 3
Testing a continuity plan follows a logical sequence of steps. The process begins by defining the purpose and approach of the test. Once the objective is clear, the team structures the test details. The actual test is then conducted according to the established framework. Finally, results are analyzed to identify weaknesses and determine if the plan requires any modifications.

**54.** (C) Routine, planned server maintenance downtime.
Computing disasters are categorized by their unplanned and disruptive nature. Natural events, accidents, and deliberate malicious actions all constitute disasters because they interrupt normal operations unexpectedly. Routine, planned downtime for server maintenance is an expected operational activity. It does not qualify as a disaster since it is scheduled and managed to minimize impact on business functions and critical services.

**55.** (A) A junior official must be designated as the Head of BCP activity or function.
RBI guidelines emphasize that business continuity is a critical function requiring high-level oversight. Therefore, a senior official should be designated as the head of the BCP activity. The organizational structure should also include crisis management teams in each department. Furthermore, Indian banks are required to report significant frauds to the Audit Committee to ensure appropriate governance and executive awareness.

**56.** (A) Identifying critical business functions and the specific timeframes in which they must be fully restored.
The most critical result of a business impact assessment is the identification of essential business functions and their restoration timeframes. This analysis determines the priority for recovering different systems based on their importance to organizational survival. By understanding these timeframes, management can allocate resources effectively. This ensures that the most vital services are restored first, minimizing the overall impact.

Click Here to Buy book on Amazon

**57.** (A) Only (I), (II), and (III)
Effective disaster avoidance requires a detailed inventory of all hardware used by the organization. Key details include the model and serial number of each piece of equipment to ensure accurate replacement. Information about alternate vendors and the current availability of replacement hardware is also critical. While facility planning might need physical dimensions, weight is not a primary recovery factor.

**58.** (A) Change management procedures are completely irrelevant in Phase 7.
Phase seven focuses on the ongoing maintenance of business continuity plans. It is critical that these plans are updated to reflect any changes in the operating environment. This process requires revising existing change management procedures to include recovery plan maintenance. Suggesting that change management is irrelevant is incorrect, as failing to sync plans with environmental changes would render the strategy obsolete.

**59.** (B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
Annual reviews and updates are necessary to maintain the effectiveness of business continuity plans as environments evolve. It is also a regulatory requirement for a copy of the board-approved BCP to be forwarded to the RBI annually. While both statements represent important compliance and management tasks, the requirement to send the plan to the regulator is not the underlying reason.

**60.** (B) It increases customer confidence in the organization's ability to respond to incidents.
Maintaining an ISO 22301-compliant system significantly enhances an organization's corporate reputation. It serves as an international certification that demonstrates the business's commitment to resilience and its ability to respond to incidents. This formal recognition increases customer confidence in the organization's stability. Clients are more likely to trust a company that has proven, standardized procedures for maintaining service levels during disruptions.

**61.** (C) Putting data "out of reach" via multiple tape generations
Protecting data from internal sabotage requires measures that prevent a malicious actor from altering both primary data and backups. Taking data "out of reach" by maintaining multiple generations of backups on physical tapes provides this protection. Unlike mirrored disks, which replicate changes immediately, offline tapes create a break. This ensures that an embezzler cannot easily destroy historical records stored safely.

**62.** (A) 4, 2, 1, 3
The SANS Institute defines a structured process for responding to security incidents. The cycle begins with preparation to ensure the organization is ready for an event. When an incident occurs, the next step is identification to confirm the nature of the threat. This is followed by containment to limit damage and eradication to remove the root cause before recovery.

**63.** (A) A destructive virus in production data will immediately replicate to the mirrored backup environment.
Mirrored systems provide excellent redundancy for hardware failures, but they present a specific risk during malware attacks. Because data is replicated instantly between the production environment and the mirror, a destructive virus will be copied to the backup immediately. Without a "break in the stream," such as an offline backup, the organization loses both primary and mirrored data simultaneously.

**64.** (C) Effective incident response is critical for minimizing operational, legal, and reputational risks.
The Basel Committee emphasizes that incident response is essential for managing various risks in electronic banking. Effective response mechanisms help minimize operational, legal, and reputational damage following a security breach. Banks should develop teams with authority to act in emergencies and establish processes for collecting forensic evidence. Proper post-incident reviews are also necessary to improve future resilience and maintain compliance.

NODIA

**65.** (A) A fully redundant environment allowing for recovery and restoration within seconds or minutes.
Hot site replication is a high-availability disaster recovery strategy. It involves maintaining a fully redundant data center environment where data is replicated in real-time from the primary site. This configuration allows for the restoration of business operations within seconds or minutes of a failure. While more expensive, it provides the fastest recovery time for organizations with critical, time-sensitive processing needs.

**66.** (A) It identifies weaknesses in the plan and validates the ability to recover specific business applications.
Theoretical success is no guarantee of real-world recovery. Testing disaster recovery plans is essential because it identifies specific weaknesses and gaps in procedures. These exercises validate the organization's ability to restore critical applications and data within required timeframes. By uncovering issues during a test, the organization can adjust plans before an actual disaster occurs, significantly increasing the likelihood of success.

**67.** (A) P-1, Q-2, R-3, S-4
Backup schedules are designed to balance data protection with operational efficiency. Full backups, capturing all data, are typically performed on a weekly basis. Incremental backups, saving only changed data, are done daily to minimize processing time. Selective backups might be conducted monthly for archival purposes. Continuous replication models provide real-time data duplication across distributed systems, ensuring the highest level of availability.

**68.** (B) Structured Walk Through Test is a live operational failover to a Hot Site.
Different types of disaster recovery tests serve various validation purposes. A read-through test involves document review, while a parallel test involves relocating personnel and implementing site activation. A structured walk-through is a tabletop exercise where team members discuss their responses to a scenario; it is not a live operational failover. Live failovers are much more complex and involve site activation.

**69.** (A) Only (I), (II), (IV), and (V)
A well-defined incident response plan offers several benefits. It streamlines forensic analysis and hastens recovery times, minimizing the duration of damage. Furthermore, it increases the confidence of shareholders and executives by demonstrating a proactive approach to security. While it helps manage reputation, the goal is to minimize negative publicity. These plans are vital for reducing the overall impact of incidents.

**70.** (C) P-2, Q-1, R-4, S-3
Disaster recovery strategies vary in cost and recovery speed. A cold site is the lowest cost solution where hardware is optional and must be brought in. A warm site requires hardware to be purchased or leased, with recovery taking hours. Hot sites provide high-end solutions with fast recovery. A mirrored environment is fully redundant and offers almost immediate restoration.

**71.** (B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
Automation in incident response allows businesses to maintain reliable, round-the-clock security monitoring and reaction. Modern cyber threats happen at speeds that make manual response difficult, as human intervention involves a time lag. While both statements highlight the benefits and challenges of different response methods, the time lag of manual tasks is a reason to adopt automation, not an explanation.

**72.** (B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
Storing media off-site provides geographic diversity, ensuring that a single event like a flood does not destroy both the primary site and the backups. Taking data off-line by creating a physical break in the data stream protects against viruses that would replicate across a network. Both are valid strategies, but protection against viruses is separate from geographic safety.

**73.** (C) Orchestration
The SANS Institute's incident response framework consists of six specific phases: preparation, identification, containment, eradication, recovery, and lessons learned. These

Downloaded from www.pdf.tube

seven creates a maintenance program to keep plans updated as the environment changes. Finally, phase eight covers the initial testing and implementation where the plan is adjusted.

**41.** (B) Only (I), (II), (IV), and (V)
A robust backup model for disaster prevention includes several specific steps. Organizations must determine the time needed for recovery and implement a classic distributed backup model. Using automatic tape verification ensures that data was written correctly to the media. Furthermore, backup copies must be stored off-site in a safe, dry, and dust-free environment. These measures protect data integrity consistently.

**42.** (C) The maximum duration a business unit can operate without access to systems, services, and core facilities.
In the context of a business impact assessment, the term "pain threshold" refers to a critical survival metric. It represents the maximum duration that a specific business unit can continue its operations without access to essential systems, services, or facilities. Identifying this threshold helps organizations prioritize the recovery of functions. It ensures time-sensitive operations are restored before irreparable damage occurs.

**43.** (B) P-3, Q-4, R-2, S-1
Business continuity management components cover various organizational needs. The methodology often utilizes international standards like ISO 22301 for best practices. Maintenance and re-assessment involve annual reviews to ensure effectiveness. Procedural aspects include setting up backup sites for critical systems. Finally, infrastructural aspects focus on maintaining basic amenities, such as electricity and water, which are necessary for operations.

**44.** (D) It strictly prohibits the use of third-party evaluations of an organization's security posture.
ISO 22301 is an international standard that outlines the requirements for a best-practice business continuity management system. It helps organizations protect their income streams and maintain service levels after a disaster. Contrary to the incorrect statement, the standard does not prohibit third-party evaluations. In fact, third-party certification is a common way for businesses to demonstrate their resilience and compliance.

**45.** (D) Assertion (A) is false, but Reason (R) is true.
Disaster avoidance involves implementing high availability, redundancy, and failover mechanisms to reduce the likelihood of a crisis. However, it is not a foolproof solution. No matter how many preventive heritage measures are in place, they cannot provide absolute protection against every possible form of damage, such as catastrophic natural events. Therefore, avoidance is a critical layer of defense but not infallible.

**46.** (C) Assertion (A) is true, but Reason (R) is false.
Phase two of the business continuity methodology focuses on reducing the possibility of a disaster through vulnerability assessment. This proactive approach is economically sound because preventing a crisis is generally less expensive than dealing with its consequences. The suggestion that organizations should focus primarily on minimizing the impact after an event is incorrect. Effective planning emphasizes prevention as much as recovery.

**47.** (B) It provides absolutely foolproof protection from all types of damage, including human malice.
Disaster avoidance encompasses steps an institution can take to respond effectively to various events. It utilizes techniques like high availability, redundancy, and failover to ensure resilience. While these activities are cost-effective and vital for security, they do not provide absolutely foolproof protection from all types of damage. Risk can be significantly reduced, but some level of vulnerability always remains.

**48.** (A) Only (I), (II), and (III)
Phase five of the methodology focuses on plan development. Key activities include defining and documenting the recovery plan components and upgrading data processing operating procedures. Organizations also negotiate vendor contracts for recovery services during this stage. While testing is a critical part of the overall methodology, the initial tests and modifications are associated with phase eight rather than plan development.

NODIA

Automated systems are necessary to provide the immediate response required for modern cyberattacks. Relying solely on manual processes leaves an organization vulnerable.

**82.** (C) Both (I) and (II)
Robust data protection involves both geographic and logical separation of backups. Taking data off-site places physical distance between the data center and the storage facility, protecting against local disasters. Taking data off-line creates a logical break that prevents mirrored systems from automatically replicating corrupted files. Together, these strategies ensure that at least one clean, physical copy of data remains safe.

**83.** (D) Up to 24 hours
A warm site is a disaster recovery solution that provides a middle ground between cold and hot sites. It typically has necessary infrastructure and some pre-installed hardware, but it requires data to be restored from backups. Because of the time needed to transport media and complete the restoration, the recovery time for a warm site is generally within twenty-four hours.

**84.** (C) Routine hardware redundancy disk mirroring
A security incident is characterized by an event that compromises or threatens the operations and data of a system. Unauthorized access, physical damage, and the presence of viruses are all clear examples of security incidents. In contrast, routine hardware redundancy through disk mirroring is a normal operational process designed to prevent an incident from causing downtime. It is a protective control.

**85.** (C) An event that compromises or potentially compromises the operation of core systems or data assets.
In information security, an incident is defined as any event that compromises, or has the potential to compromise, the operation of core systems or data assets. This includes unauthorized access, data breaches, and malicious software infections. Identifying these events is the first step in the response process. Distinguishing between normal variations and significant security threats allows for structured intervention.

**86.** (B) 5 to 7 days
A cold site is a basic disaster recovery facility that provides space and power but lacks pre-installed computer hardware or data. Following a disaster, the organization must acquire, install, and configure all necessary equipment before data restoration can begin. Due to these logistical requirements, the typical recovery time for a cold site strategy in a medium-sized bank ranges from five to seven days.

**87.** (C) Hot Site Replication - Lowest Cost Solution
Disaster recovery strategies have a direct relationship between cost and recovery speed. Cold sites are the least expensive because they have minimal pre-installed equipment. Hot sites, which provide a fully redundant environment and almost immediate restoration, are among the most expensive solutions due to the high cost of maintaining duplicate hardware and real-time replication. Labeling it lowest-cost is factually incorrect.

**88.** (B) To provide protection against online attacks and viruses that mirrored systems cannot defend against.
Modern data protection must account for threats that bypass standard hardware redundancy. While mirrored systems protect against disk failures, they cannot stop a virus from replicating to the backup. Keeping multiple generations of data on physical tapes at a remote location puts that data “out of reach” of online attacks. These offline tapes provide a clean point-in-time version for restoration.

**89.** (B) Eradication removes the root cause, while Recovery safely returns systems to the production environment.
The SANS incident response framework distinguishes between technical removal and operational restoration. Eradication is the phase focused on identifying and removing the root cause of the security incident, such as deleting malware. Recovery is the subsequent phase where systems are safely returned to the production environment and normal operations resume. This orderly progression ensures the threat is eliminated before restoration.

Click Here to Buy book on Amazon

proactive response enables the system to triage alerts efficiently in real-time, allowing security analysts to focus.

**107.** (D) Warm Site Replication
The recovery strategy described involves a secondary site that requires hardware leasing and has a recovery time of eight hours. This characterizes a warm site replication strategy. Warm sites provide a middle ground where some infrastructure is present, but full operational capacity requires additional steps like data restoration. This is faster than a cold site but does not offer near-instantaneous recovery.

**108.** (A) It transfers residual cyber risk that cannot be addressed by avoiding, mitigating, or reducing.
Cyber insurance is used as a financial tool within a risk management framework to transfer residual risk. This is the risk that remains after an organization has implemented controls to avoid, mitigate, or reduce potential threats. It provides financial protection against immediate costs of an attack, such as data recovery. It does not replace security controls but rather complements them by addressing impact.

**109.** (D) Phase 3 - Business Impact Assessment (BIA)
The "pain threshold," which defines the maximum time a business unit can survive without its systems, is assessed during the Business Impact Analysis (BIA). In the business continuity methodology, this is conducted during phase three. This phase is critical because it identifies recovery priorities. By understanding these thresholds early, the organization can develop appropriate strategies to ensure functions are restored timely.

**110.** (D) All (I), (II), and (III)
Standard cyber insurance policies are designed to cover various costs associated with responding to a ransomware attack. This includes the expenses for recovering lost or encrypted data and hiring forensic experts to investigate the incident. The costs associated with determining exactly what happened during the breach are also typically covered. These provisions help an organization manage the significant financial burden of security events.

**111.** (D) Risk transferring via cyber insurance
When a bank uses an insurance policy to cover the costs of hiring forensic professionals, it is employing a risk treatment method known as risk transfer. By paying a premium to an insurance provider, the bank shifts the potential financial burden of an incident to a third party. This does not eliminate technical risk but ensures the bank has financial resources for recovery.

**112.** (D) All (I), (II), and (III)
Automated incident response through SOAR provides several key features. It addresses the complexity of coordinating people, processes, and technology manually. By automating repetitive tasks, the system expedites response with minimal human intervention. Furthermore, it enables a proactive and systemic response to security breaches. These capabilities are essential for managing the high volume and speed of modern cyber threats effectively and consistently.

**113.** (C) Law enforcement strongly encourages paying ransoms to quickly recover operational capacity.
Contrary to the incorrect statement, law enforcement agencies do not encourage paying ransoms to cyber criminals. They strongly advise against it because it funds criminal activities and encourages more attacks. While some insurance policies might cover ransom costs, the security industry as a whole discourages this practice. Organizations are instead urged to focus on preventive controls and robust data recovery procedures.

NODIA

**114.** (B) Incremental backup
An incremental backup is a data protection strategy where only the files that have changed since the last backup are saved. This approach is much faster than performing a full backup every day, as it reduces the volume of data being processed. In the given scenario, the administrator uses this method to prioritize speed. It ensures recent changes are captured efficiently.

**115.** (A) Disk Duplexing
The administrator is implementing disk duplexing, a redundancy technique where two hard disks operate in tandem, each with its own separate controller circuitry. This configuration is more robust than simple mirroring because it eliminates the single point of failure at the

**98.** (A) A vulnerability due to improper design and weakness in operations
In security and continuity planning, a vulnerability is any weakness that can be exploited by a threat. Placing a computer center on the ground floor in a flood-prone area represents an inherent weakness in the design and implementation of the facility. This improper design makes the system vulnerable to environmental disasters. Identifying such weaknesses is a core part of vulnerability assessment.

**99.** (B) RAID 5 array
RAID level 5 is a storage technology that provides both performance and fault tolerance. It requires a minimum of three hard drives and uses distributed parity to protect data. A key advantage is that it often allows for "hot swapping," where a failed drive can be replaced while the server continues to run. This technology is an effective way to maintain high availability.

**100.** (C) Ignoring
Standard risk management frameworks provide several ways to address cyber risk. Organizations can avoid the risk by not engaging in certain activities, mitigate or reduce the risk through security controls, or transfer the risk through insurance. Ignoring the risk is not a recognized method of risk treatment. Failing to address known vulnerabilities leaves the organization exposed to significant financial and operational damage.

**101.** (A) Because it encourages cyber criminals to commit more attacks.
Law enforcement and security professionals advise against paying ransoms because it fuels the criminal ecosystem. By paying, organizations demonstrate that ransomware is a profitable business model, which encourages attackers to target more victims. Furthermore, there is no guarantee that the criminals will actually provide the decryption keys. Focusing on recovery from backups is a more reliable and ethically sound strategy.

**102.** (A) An employee deliberately triggers a fire alarm as a prank without network interaction.
SOAR systems are designed to coordinate responses to security incidents involving digital networks and IT systems. Examples include managing malware infections, blocking command-and-control communications, and responding to ransomware alerts. An employee triggering a fire alarm as a physical prank without network interaction does not involve digital systems managed by SOAR. This incident would be handled by physical security and human resources.

NODIA

**103.** (B) Parallel Test
A parallel test is specifically designed to validate the organization's ability to relocate its personnel and operations to an alternate site. During this type of test, the recovery team physically moves to the secondary location and implements site activation procedures as if a real disaster occurred. This differs from simpler tabletop exercises because it involves actual physical relocation and the performance of duties.

**104.** (D) To assist in determining what occurred during an attack and resolving the technical problem.
Cyber insurance policies often include coverage for hiring forensic cybersecurity professionals during an investigation. Their role is to provide technical expertise to determine exactly how an attack occurred and what systems were affected. They assist the organization in resolving the problem and preventing future breaches. This specialized knowledge is essential for a thorough incident response and for satisfying various regulatory requirements.

**105.** (C) Eradication
According to the SANS Institute framework, the phase focused on removing the root cause of an incident is known as eradication. In the given scenario, the incident response team identifies the infected server and removes it from the production environment to stop the threat. This action directly targets the source of the ransomware, ensuring it is completely eliminated before moving to recovery.

**106.** (A) P-2, Q-3, R-4, S-1
SOAR systems utilize several distinct capabilities to manage incidents. Orchestration involves coordinating actions across multiple security tools and IT systems. Automation refers to translating playbooks into commands the system can execute. SOAR integration uses threat intelligence to detect malicious traffic automatically. Finally, a

phases provide a comprehensive lifecycle for managing security events. While orchestration is a modern technical capability used within these phases to automate actions, it is not one of the six standard phase names defined in the original SANS framework.

**74.** (B) Crisis mechanism - Identify a crisis as soon as it occurs, assess materiality, and control reputation risk.
The Basel Committee provides recommendations for managing risks in electronic banking. One key function is establishing a crisis mechanism that can identify a crisis immediately, assess materiality, and take steps to control reputation risk. Contrary to other options, banks should preserve forensic evidence and ensure incident response teams have authority to act. Recovery plans should consider various geographic and technical scenarios.

**75.** (A) Only (I), (II), and (III)
According to the Basel Committee, banks should develop several critical functions for effective incident response. These include mechanisms to assess the impact of a crisis and protect the bank's reputation. Incident response teams must be trained to interpret technical data accurately. Additionally, a process for collecting and preserving forensic evidence is essential. Organizations should conduct reviews to learn from incidents.

**76.** (C) Only (I), (III), and (IV)
Managing backup performance requires understanding different tape technologies. The standard overnight backup window may not be short enough for modern recovery requirements. Tape management software helps by placing mission-critical data on high-performance devices. Conversely, ultra-high capacity drives are often slower and better suited for archival data. Therefore, high capacity does not automatically equate to high performance in recovery scenarios.

**77.** (D) ISO 27002 establishes strict mandatory certification protocols that supersede ISO 22301.
ISO 27001 and ISO 27002 are complementary standards focused on information security. ISO 27001 provides compliance requirements for certification, while ISO 27002 offers detailed best practices for incident response. Neither of these standards supersedes ISO 22301, which focuses specifically on business continuity management. They address different aspects of organizational resilience and are often used together in a comprehensive program.

**78.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Internal sabotage is difficult to carry out against vaulted tape data because it requires physical access to a secure location. Unlike online systems where data can be altered remotely, physical tapes in a vault are protected by multiple layers of security. An embezzler would need to breach these physical measures, making it nearly impossible to modify data without leaving evidence.

**79.** (B) Containment - Finding the root cause of the incident and removing affected systems
Each phase of the SANS incident response plan has a distinct objective. Preparation readies staff, and identification confirms the incident. Containment is specifically focused on limiting damage and preventing the threat from spreading. The task of finding the root cause and removing affected systems actually belongs to the eradication phase. Misunderstanding these distinctions can lead to an ineffective and unsuccessful response.

**80.** (B) P-3, Q-1, R-4, S-2
Disaster recovery testing involves several levels of complexity. A read-through test is a simple document review by team members. A structured walk-through is a tabletop exercise where a scenario is discussed. In a simulation test, members develop a response to a hypothetical event. Finally, a parallel test is a rigorous exercise that involves relocating personnel to an alternate site.

**81.** (C) The time lag involved cannot guarantee an immediate response required for most cyber incidents.
Cyber incidents often occur and propagate at extremely high speeds, requiring an almost instantaneous reaction to prevent widespread damage. Manual incident response is inherently flawed because the time lag involved in human detection and intervention is too great.

Downloaded from www.pdf.tube

controller level. Additionally, dual controllers allow for performance optimizations like split seeks, where the system can handle multiple read requests simultaneously.

**116.** (D) It isolates threats by integrating with endpoint antivirus and automatically quarantining infected systems.
Orchestration in a SOAR system enables different security tools to work together in a coordinated response. During a virus detection event, the system can automatically integrate with endpoint antivirus software to isolate the threat. It can then quarantine infected systems and update network firewalls. This coordinated action happens much faster than manual intervention, effectively containing the threat and preventing its spread.

**117.** (D) Automation
The scenario demonstrates the automation capability of a SOAR system. Automation specifically refers to the system's ability to execute commands and workflows without human intervention. By translating instructions in a security playbook directly into firewall commands to block a malicious IP, the system reacts instantly. This removes delays associated with manual responses and ensures a rapid defense against detected ransomware attacks.

**118.** (D) It covers the immediate costs of a cyberattack, including data recovery and investigation expenses.
Cyber insurance is designed to protect organizations from the financial impact of a security breach. It typically covers the immediate costs associated with a cyberattack, including data recovery expenses and the fees for technical investigations. Some policies also cover legal fees and public relations efforts. By providing these financial resources, cyber insurance enables an organization to restore its operations more quickly.

**119.** (A) Data safes designed for magnetic media
Magnetic media are highly sensitive to environmental factors. To protect them from extreme heat, humidity, and contaminants, they must be stored in specialized data safes. These safes are built to maintain a stable internal environment even during a fire, which standard fire-resistant filing cabinets cannot do for magnetic media. Proper storage is essential for ensuring that backups remain readable.

**120.** (A) P-4, Q-3, R-1, S-2
Various international standards provide frameworks for organizational resilience and security. ISO 22301 focuses on best practices for business continuity management systems. ISO 27001 outlines the compliance requirements for information security certification. ISO 27002 provides detailed guidelines for incident response and internal investigations. Finally, the Basel Committee reports offer specific guidance on risk management for electronic banking for financial institutions.

**121.** (D) The Board
According to RBI requirements, the maintenance and re-assessment of business continuity plans are critical governance tasks. Any updates to the BCP must receive formal approval from the Board of Directors. This ensures that senior leadership is aware of and supports the organization's resilience strategies. Once approved, a copy of the plan is forwarded to the RBI annually for their perusal.

NODIA

**122.** (C) The Audit Committee of the Board
In the Indian banking industry, regulatory guidelines require that significant internal financial frauds be reported to high-level oversight bodies. For a fraud amounting to 1.5 crore, which exceeds the reporting threshold, the bank must officially report the incident to the Audit Committee of the Board. This ensures that the bank's directors are informed of major risks and oversight activities.

**123.** (C) ISO 22301
ISO 22301 is the formally recognized international standard for business continuity management systems. Pursuing certification under this standard allows an organization to demonstrate its resilience and operational stability to regulators and customers. This certification proves that the bank has implemented a best-practice framework for maintaining service levels during disasters. It provides a competitive advantage by building trust in resilience efforts.

of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2024**

**22.** Which of the following is an exception to the basic areas of an IT audit scope?
(A) Development of an IT contingency plan
(B) Setting organizational macroeconomic policies
(C) Physical environment in which computers operate
(D) Review of user applications and end-user access

**May/June 2017**

**23.** A bank wants to deploy an advanced data encryption solution across all its regional offices to maintain data integrity. The software costs $500,000, while the estimated maximum financial benefit from preventing data distortion is $300,000. Under the principles of System Audit, what is the most logical recommendation?
(A) Implement the system immediately to ensure absolute data integrity for the bank
(B) Implement the system only at the head office to reduce costs for the branch
(C) Proceed with implementation since data integrity should not be evaluated on a cost-benefit basis
(D) Reject the system as the implementation cost exceeds the resulting benefits

**Oct/Nov 2005**

**24.** Which of the following is an exception to the qualitative or quantitative parameters used by auditors to evaluate the effectiveness of the system?
(A) Improvement in Task Accomplishment
(B) Organizational Effectiveness
(C) Technical and Economic Effectiveness
(D) Depreciation of the office real estate

**May/June 2020**

**25.** Identify the incorrect statement regarding concurrent audit techniques.
(A) ITF - Integrated Test Facility for live testing
(B) Concurrent Arithmetic and Analytical Test Tools
(C) SCARF - System Control Audit Review File
(D) CIS - Continuous and Intermittent Simulation system

**Oct/Nov 2015**

**26.** Which of the following statements correctly describes "Maintaining process integrity"?
(A) It ensures that the organizational database is shared between various offices with high efficiency
(B) It focuses on evaluating the specific characteristics of the end-users and their behaviors
(C) It implies that organizational data is kept complete, accurate, and without any distortion
(D) It ensures uniform, uncorrupted computer system processing

**May/June 2013**

**27.** Consider the following statements regarding the objectives of security and control measures:
I To prevent data loss and loss of costly computer resources.
II To encourage computer errors for testing purposes.
III To prevent incorrect decisions due to incorrect or fraudulent data.
Which of the above statements are correct?
(A) (I) and (II)
(B) (I) and (III)
(C) (II) and (III)
(D) (I), (II), and (III)

**Oct/Nov 2021**

**28.** Match the steps of the Planning Process in a System Audit (List-I) with their corresponding actions (List-II).
List I: (Steps of Planning Process)
P. Step 1
Q. Step 2
R. Step 3
S. Step 4
List II: (Actions)
1. Determine the most effective and efficient audit strategy
2. Document the planned audit strategy
3. Review the latest Audit Report and take necessary steps
4. Obtain a preliminary understanding of the system to be audited and document it properly
(A) P-3, Q-4, R-1, S-2
(B) P-4, Q-3, R-2, S-1
(C) P-3, Q-1, R-4, S-2
(D) P-1, Q-2, R-3, S-4

Click Here to Buy book on Amazon

# CHAPTER 18
# Information System Audit

May/June 2021

**1.** What is the most appropriate reason why System Audit is important in a computerized environment?
(A) It eliminates the need for any manual human intervention in business operations
(B) It ensures that traditional methods of frauds are completely replaced by IT related frauds
(C) It replaces the senior Board of Directors in the official decision-making process
(D) It ensures IT systems are protected, reliable, and properly managed

Oct/Nov 2014

**2.** Which of the following assures whether the audit version of the software is an authorized one or not?
(A) Source Code Comparison
(B) Test Data approach
(C) Object Code Comparison
(D) Integrated Test Facility

May/June 2023

**3.** In the context of maintaining data integrity, an organization incurs expenditure to ensure data is complete and accurate. Which of the following represents the primary economic principle guiding this expenditure?
(A) The cost must be minimized regardless of the data quality outcome
(B) The benefits must be ignored if the statutory requirement is met
(C) The cost must not be greater than the benefits arising out of it
(D) The expenditure must match the IT budget exactly

Oct/Nov 2025

**4.** Consider the following statements regarding the benefits of Audit Software:
I They are independent of the system being audited.
II They use a read-only copy of the file to avoid any corruption of an organization's data.
Which of the above statements is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

NODIA

May/June 2007

**5.** Consider the following statements about Generalized Audit Software:
I It allows auditors to gain access to the data maintained in computerized media.
II It includes functions such as File Access, Arithmetic, Stratification, and frequency analysis.
III It provides a direct way of examining the program source codes for unauthorized coding.
Which of the above statements are correct?
(A) (I) and (II)
(B) (II) and (III)
(C) (I) and (III)
(D) (I), (II), and (III)

Oct/Nov 2009

**6.** Consider the following statements about Environmental Controls:
I UPS Systems and Voltage Stabilizers ensure smooth and uninterrupted supply of power.
II Fire Control includes the installation of Smoke Detectors and Fire Extinguishers.
III The System Room temperature and humidity must be controlled.
IV Pest Control and Water Damage Control are considered Environmental Controls.
V Logical security using passwords is a primary component of Environmental Controls.
Which of the above statements are correct?
(A) (I), (II), (III), and (IV)
(B) (I), (II), IV), and (V)
(C) (II), (III), (IV), and (V)
(D) (I), (II), (III), and (V)

May/June 2016

**7.** The concept of System Audit essentially refers to which of the following?

(A) An audit of the manual human resource management system
(B) An audit of the computer system
(C) An audit limited to the financial accounting ledgers
(D) An audit of the external vendor relationships

**Oct/Nov 2018**

**8.** Identify the correct pair connecting the audit technique to its primary characteristic.
(A) Test Data - Examines the quality of data produced by a program directly from the live database
(B) Program Code Comparison - Compares program codes of the audit version with the standard version
(C) Generalized Audit Software - Direct way of examining program source codes
(D) Concurrent Audit Techniques - Relies solely on manual questionnaires and control flow charts

**May/June 2012**

**9.** Identify the incorrect statement regarding the collection and evaluation of evidences in a System Audit.
(A) Concurrent Audit Techniques are used when an auditor needs to collect evidences and evaluate them instantaneously
(B) Audit software corrupts the organization's data by using a write-enabled copy of the file during sampling
(C) Manual techniques for collecting evidences include Interviews, Questionnaires, and Control Flow Charts
(D) Evaluation of Asset Safeguarding and Data Integrity Capability is done simultaneously

**Oct/Nov 2006**

**10.** Arrange the following phases of an IS audit in the correct chronological sequence:
1. Gather information on the relevant IT controls
2. Establish the objectives and scope
3. Develop a plan to achieve the objectives
4. Perform audit tests using CAATs
5. Reports on the IS audit findings
6. Follow up

(A) 2, 3, 1, 4, 5, 6
(B) 1, 2, 3, 4, 5, 6
(C) 2, 1, 3, 5, 4, 6
(D) 3, 2, 1, 4, 6, 5

**May/June 2019**

**11.** A data center recently experienced corrupted data files due to a sudden fluctuation in the utility grid. To avoid such occurrences in the future, the IS Auditor recommended specific Environmental Controls. Which set of mechanisms should the organization implement?
(A) Dead Man's Doors and CCTV
(B) SCARF
(C) Biometrics technology, encrypted passwords, and multi-factor systems
(D) UPS systems, voltage stabilizers, and redundant power infrastructure

**Oct/Nov 2022**

**12.** Identify the incorrect statement regarding Effectiveness Auditing and Efficiency Auditing.
(A) Effectiveness auditing evaluates whether the computer system is achieving the goals of the organization
(B) Efficiency auditing focuses on whether efficiency has been increased after adopting the computer system
(C) Efficiency auditing evaluates user characteristics before a system has been running
(D) Efficiency auditing reveals the hardware and software adequacy for the specific system

**May/June 2018**

**13.** Computer Aided Audit Tools and Techniques (CAATTs) generally refers to:
(A) Any computer program utilized to improve the audit process, like data software
(B) Any manual checklist or document utilized to improve the overall audit process
(C) The physical security hardware installed on doors, such as a dead man's door
(D) The biometric access control devices used for verifying human identity

**Oct/Nov 2016**

**14.** Consider the following statements about Computer Aided Audit Tools and Techniques (CAATTs):
I CAATTs refer to any computer program utilized to improve the audit process.
II Data analysis and extraction tools are considered part of CAATTs.
III Databases such as MS Access are excluded

Downloaded from www.pdf.tube

from CAATTs.
IV Business intelligence tools like Crystal Reports and Business Objects can act as CAATTs.
Which of the above statements are correct?
(A) (I), (II), and (III)
(B) (II), (III), and (IV)
(C) (I), (II), and (IV)
(D) (I), (III), and (IV)

**May/June 2014**

**15.** Consider the following types of controls in a computerized environment:
I Access Controls
II Input Controls
III Communication Controls
IV Database Controls
Which of the above statements correctly identifies these controls?
(A) (I), (II), and (III)
(B) (I), (III), and (IV)
(C) (II), (III), and (IV)
(D) (I), (II), (III), and (IV)

**Oct/Nov 2007**

**16.** Which of the following is NOT one of the four basic objectives of a System Audit?
(A) Maximizing marketing efficiency
(B) Safeguarding the assets
(C) Maintaining data integrity
(D) Maintaining process integrity

**May/June 2025**

**17.** What is the most appropriate reason for implementing a multi-layer security strategy in a computerized environment?
(A) Multi-layer security is more effective than a single barrier in networking
(B) To increase the hardware processing speed of the main computer architecture
(C) To bypass the need for a Disaster Prevention and Recovery Plan
(D) To eliminate the organizational need for a dedicated internal audit department

**Oct/Nov 2019**

**18.** Consider the following statements regarding the Audit Organization:
I Internal Auditors understand the system and procedures better but might be influenced by the management.
II External Auditors will be impartial and are not influenced by management, and require minimal time to understand the systems.
Which of the above statements is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**May/June 2009**

**19.** Which of the following is NOT a function performed using Computer-Assisted Audit Techniques (CAATs)?
(A) Evaluating data accuracy and completeness
(B) Performing analytical review procedures
(C) Validating records with actual entities
(D) Designing the physical IT infrastructure

**Oct/Nov 2011**

**20.** The following question consists of two statements: Assertion (A) and Reason (R). Select the correct answer using the codes given below.
Assertion (A): Program Source Code Review identifies erroneous code, unauthorized code, and non-standard code.
Reason (R): Generalized Audit Software is designed primarily as a direct way of examining program codes rather than examining the quality of data.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2010**

**21.** The following question consists of two statements: Assertion (A) and Reason (R). Select the correct answer using the codes given below.
Assertion (A): Dead Man's Door effectively reduces the risk of piggybacking.
Reason (R): It uses a pair of doors where the first entry door must close and lock with only one person permitted in the holding area before the second door operates.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation

NODIA

(A) All users should be given rights to access the Operating System to improve productivity
(B) Review and Removal of Dormant Users requires IDs of transferred users to be kept active for six months
(C) Activity logs are kept secret from controllers to ensure individual user privacy
(D) Terminal restriction limits a user to working on one specific machine only

**Oct/Nov 2022**

**53.** Identify the correct pair regarding the security controls.
(A) Processing Controls - Prevents preparation of false Input Forms
(B) Communication Controls - Ensures clean and uninterrupted power
(C) Database Controls - Uses backups to maintain data integrity
(D) Output Controls - Ensures that the system OS is policy-hardened

**May/June 2018**

**54.** Which of the following are the two primary types of audit trails that must be maintained in a system?
(A) Hardware audit trail and Software audit trail
(B) Manual audit trail and Automated audit trail
(C) Accounting audit trail and Operations audit trail
(D) Input audit trail and Output audit trail

**Oct/Nov 2016**

**55.** The following question consists of two statements: Assertion (A) and Reason (R). Select the correct answer using the codes given below.
Assertion (A): Disaster recovery plans should include Risk Assessment and Business Impact Analysis.
Reason (R): The purpose of DPRP is to identify probable disasters that may affect the system and find out methods to prevent them or minimize their effects.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2014**

**56.** Which of the following represents the standard requirements for minimum password length and complexity to ensure robust logical security?
(A) At least 8 characters with upper/lower cases, numbers, and special symbols
(B) At least 6 characters including specific upper case and numeric characters
(C) At least 10 characters with only numeric values
(D) At least 4 characters with one special character

**Oct/Nov 2007**

**57.** Identify the incorrect statement regarding the audit trail in the communication subsystem.
(A) Public network owners always supply required audit trail information
(B) The audit trail must allow message tracing through every network node
(C) It maintains chronology from sender dispatch until the receiver obtains it
(D) Audit trail information is needed if a message is lost in the network

**May/June 2025**

**58.** Match the password security features (List-I) with their descriptions (List-II).
List I: (Security Features)
P. Password Expiry Date
Q. Grace Login
R. Unique Password
S. Minimum Password Length
List II: (Descriptions)
1. Whether users will be allowed to use the already used password
2. Compels users to change their passwords after a certain date
3. Forces users to use a password of a certain number of digits
4. Specifies how many times users are allowed to login after password expiry
(A) P-2, Q-4, R-1, S-3
(B) P-4, Q-2, R-3, S-1
(C) P-1, Q-3, R-2, S-4
(D) P-3, Q-1, R-4, S-2

**Oct/Nov 2019**

**59.** Match the type of control (List-I) with its corresponding example/objective (List-II).

Click Here to Buy book on Amazon

May/June 2024

**29.** Identify the correct statement regarding the Test Data approach.
(A) It involves the collection of evidences online and comprehensively
(B) It compares the object codes of two different software versions
(C) It uses dummy data to test if a program contains specific processing errors
(D) It extracts and analyzes real transaction data from the corporate master file

Oct/Nov 2008

**30.** Consider the following statements regarding the tasks accomplished by combining functional capabilities of Generalized Audit Software:
I Evaluate the quality of data.
II Evaluate the quality of system processing.
III Examine the existence of entities which data purports to represent.
IV Analytical Review.
V Examine the physical hardware architecture of the database servers.
Which of the above statements are correct?
(A) (I), (II), (III), and (IV)
(B) (I), (II), (IV), and (V)
(C) (II), (III), (IV), and (V)
(D) (I), (III), (IV), and (V)

May/June 2006

**31.** Identify the incorrect statement regarding input controls.
(A) The purpose of input controls is to prevent unintentional entry of wrong data
(B) Input Controls primarily ensure the maintenance of organizational data integrity
(C) Maker-Checker allows the same person entering data to perform the final check
(D) Input forms must bear Terminal Number Stamp and initials of Data Entry Operators

Oct/Nov 2017

**32.** A data center recently experienced corrupted data files due to a sudden fluctuation in the utility grid. To avoid such occurrences in the future, the IS Auditor recommended specific Environmental Controls. Which set of mechanisms should the organization implement?
(A) Dead Man's Doors and CCTV
(B) SCARF
(C) Biometrics technology, encrypted passwords, and multi-factor systems
(D) UPS systems, voltage stabilizers, and redundant power infrastructure

May/June 2008

**33.** Which of the following best defines "Grace Login" in the context of password security features?
(A) A mechanism that automatically locks the workstation when the user is away
(B) The allowed logins for a user after their password has officially expired
(C) The restriction of user login to specific working days
(D) The rule dictating the minimum number of special characters in a password

Oct/Nov 2013

**34.** Identify the correct statement regarding the data kept in the accounting audit trail.
(A) It includes the number of errors occurring on each link
(B) It includes queue lengths at each node
(C) The log of system restarts and specific message transit times
(D) Identity of users, authentication info, and login attempt counts

May/June 2015

**35.** Identify the incorrect statement regarding the steps to ensure adequate controls at the point of input.
(A) Maker-Checker - One person enters data and checks it themselves
(B) Overlapping of roles - Avoided as far as possible
(C) Input Forms - Must bear authorized signatures from authorities
(D) Data entry validation - Prevents intentional entry of fraudulent data

Oct/Nov 2012

**36.** What is the most appropriate use of the operations audit trail data by a network supervisor?
(A) To identify network problems and reconfigure the network accordingly
(B) To identify the specific person authorizing the message dispatch
(C) To determine the cost of the hardware
(D) To evaluate the effectiveness of the Maker-

Downloaded from www.pdf.tube

**124.** (A) Yes, RBI guidelines suggest that banks should consider having unplanned BCP drills.
RBI guidelines specifically support the use of unplanned business continuity drills. These drills are designed to test the true readiness of the bank's staff and the effectiveness of its procedures under realistic, surprise conditions. By conducting these exercises without prior warning, the organization can identify genuine gaps in its response capabilities that might not be visible during a scheduled test.

**125.** (B) Procedural aspects of BCP
Under the RBI guidelines for business continuity management, establishing backup sites for critical systems falls under the category of procedural aspects. These procedures ensure that vital functions, such as payment processing, can continue even if the primary site is unavailable. This involves the tactical arrangement of alternative locations and synchronization of data. It is a key component of management.

www.nodia.in

NODIA

auditors verify computer generated transactions with the same derived manually.

Which of the above statements is/are correct?

(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**Oct/Nov 2025**

**45.** Which of the following is an exception to the data items kept in the accounting audit trail for a communication subsystem?

(A) The unique identifier of the source code being utilized
(B) Time and date at which message dispatched
(C) Number of retransmissions occurring across each network link
(D) Message sequence number

**May/June 2016**

**46.** If a 'brute force' tool can crack a 4 character password in just 4 seconds, what is the approximate time required for the same tool to crack an 8 character password?

(A) 4 minutes
(B) 10 years
(C) 4 hours
(D) 10 months

**Oct/Nov 2018**

**47.** Conceptually, what is the primary function of the operations audit trail as opposed to the accounting audit trail?

(A) The operations audit trail shows the source and nature of data that update the database
(B) The operations audit trail maintains a record of attempted or actual resource consumption within a system
(C) The operations audit trail records the unique identifier of the source code authorizing a message dispatch
(D) The operations audit trail serves solely to evaluate user passwords

**May/June 2007**

**48.** Which of the following is an exception to the objectives of Output Controls?

(A) Unauthorized alteration in the reports
(B) Ensuring that the data entering the system is correct and error-free
(C) Preventing the willful suppression of important reports or their parts
(D) Delivery of reports to unauthorized persons

**Oct/Nov 2014**

**49.** A bank assesses that a potential earthquake could heavily damage its physical IT assets. The management decides to ensure all assets are insured against this eligible risk so that they can claim the insured amount. This measure falls under which category?

(A) Controls of Last Resort
(B) Input Controls
(C) Database Controls
(D) Communication Controls

**May/June 2012**

**50.** Consider the following statements regarding Database Controls:

I Data is copied to another database or storage media like magnetic tape known as Back-Up.
II Back-Up tapes should be stored in off-site storage for safety.
III Tapes should be restored occasionally to test that they are maintained properly.
IV Anti-Virus packages are unnecessary for databases since tape backups exist.

Which of the above statements are correct?

(A) (I), (II), and (III)
(B) (I), (II), and (IV)
(C) (II), (III), and (IV)
(D) (I), (III), and (IV)

**Oct/Nov 2006**

**51.** Consider the following statements regarding the audit trail at the database system level:

I It allows management or auditor to create the time series of events that occurs when a user attempts to gain access to system resources.
II Periodically, the audit trail should be analyzed to detect any control weaknesses in the system.

Which of the above statements is/are correct?

(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**May/June 2019**

**52.** Identify the correct statement regarding logical security features.

Click Here to Buy book on Amazon

Checker process

May/June 2011

**37.** An unauthorized individual closely follows an authorized employee into a restricted System Room without using an access card. What physical security measure is specifically designed to prevent this type of breach?
(A) Dead Man's Door (Deadman doors)
(B) Biometric thumbprint reader on computer terminals
(C) Password Expiry Date
(D) Anti-Virus packages

Oct/Nov 2020

**38.** Consider the following methods by which checked outputs are preserved:
I Checked Outputs are returned to the designated official/employee.
II Outputs are sent for centralized filing and storage.
III All Outputs including 'Nil' reports are filed/bound in proper sequence.
IV Outputs are preserved for their respective periods of retention.
V Careless handling of reports is encouraged after the expiry of the retention period.
Which of the above statements are correct?
(A) (I), (II), (III), and (IV)
(B) (I), (II), (IV), and (V)
(C) (II), (III), (IV), and (V)
(D) (I), (III), and (IV), and (V)

May/June 2022

**39.** Define "Audit Trail" in the context of information system controls.
(A) A process of writing source code to optimize overall system performance
(B) The physical path taken by a network supervisor to inspect server racks
(C) The encryption of messages sent over a public network
(D) A chronological record of system events to answer queries and fulfill laws

Oct/Nov 2023

**40.** What is the most appropriate security measure to prevent sensitive menus from being accessed by unauthorized users in a menu-driven package?
(A) Using specialized system intrusion detection software packages
(B) Activating the Continuous and Intermittent Simulation
(C) Installing a Water Damage Control system
(D) Applying specific security codes for restricted menu access

Oct/Nov 2010

**41.** Consider the following data items:
I Unique identifier of each node in the network that the message traversed.
II Time and date at which each node in the network was traversed by the message.
III Queue lengths at each node.
Which of the above items might be kept in the accounting audit trail of a communication subsystem?
(A) (I) and (II)
(B) (I) and (III)
(C) (II) and (III)
(D) (I), (II), and (III)

NODIA

May/June 2005

**42.** Conceptually, what is the purpose of the "Restriction to Concurrent Connections" control?
(A) Ensuring that users connect to the production system only on official Sundays
(B) To restrict the users to a single menu in a menu-driven package
(C) Preventing users from logging in on more than one computer at a single time
(D) To delete IDs of transferred staff members

Oct/Nov 2009

**43.** In a core banking application, a junior clerk enters a transaction to transfer funds. The system requires a senior officer to authorize this transaction before it is processed. This segregation of duties is a practical implementation of which control concept?
(A) Processing Controls
(B) Maker-Checker
(C) Dead Man's Door
(D) Concurrent and Intermittent Simulation

May/June 2023

**44.** Consider the following statements regarding Processing Controls:
I The purpose of Processing Controls is to ensure that the system processes the data correctly by maintaining the integrity of the programs.
II In Processing Control through the system,

List I: (Type of Control)
P. Access Controls
Q. Output Controls
R. Environment Controls
S. Controls of Last Resort
List II: (Example/Objective)
1. Protection against careless handling of reports
2. Disaster Prevention and Recovery Plan (DPRP)
3. Water Damage Control and Pest Control
4. Biometrics Technology and Passwords
(A) P-4, Q-1, R-3, S-2
(B) P-3, Q-4, R-2, S-1
(C) P-1, Q-2, R-4, S-3
(D) P-2, Q-3, R-1, S-4

**May/June 2009**

**60.** Consider the following statements about Communication Controls:
I In the mainframe environment, data security is controlled easily by the operating system and operating system security utilities.
II In a distributed processing environment, security regarding communication relies heavily on Network Operating System (NOS).
III Networking of computers has decreased the problem of message interception.
Which of the above statements are correct?
(A) (I) and (II)
(B) (I) and (III)
(C) (II) and (III)
(D) (I), (II), and (III)

**Oct/Nov 2011**

**61.** Which of the following are the three main approaches for computer auditing?
(A) Audit before the computer, Audit over the computer, Audit after the computer
(B) System Audit, Application Audit, Network Audit
(C) Audit around the computer, Audit through the computer, Audit with the computer
(D) Internal Audit, External Audit, Concurrent Audit

**May/June 2010**

**62.** The Chief Audit Executive is forming a team to audit a newly developed complex core banking software. Recognizing that traditional financial auditors lack deep IT knowledge, the CAE recruits a specialist from the bank's own EDP department to join the team. This action directly addresses which concept?
(A) Audit competence being put together on a professional team basis
(B) Analyzing the various disadvantages of auditing around the computer
(C) Applying the logical restriction to concurrent user connections
(D) Grace Login

**Oct/Nov 2024**

**63.** The following question consists of two statements: Assertion (A) and Reason (R). Select the correct answer using the codes given below.
Assertion (A): In the "Audit around the computer" approach, logic is considered reasonable, simple to use, and familiar to auditors.
Reason (R): The auditor directly examines the internal logic and controls existing within the computer system's processing functions.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2017**

**64.** Which of the following is an exception to the activities performed during the User Procedures & Training phase?
(A) Preparation of procedures for the conversion to the new system
(B) Preparation of procedures for the operation of the new system
(C) Creating source coding and translating technical specifications
(D) Checking if the user has adequate procedure manuals and related job descriptions

**Oct/Nov 2005**

**65.** What is the most appropriate disadvantage of the "Audit around the computer" approach?
(A) It is tedious and comparisons are limited as input data changes
(B) It acquires greater confidence that data processing is accurate
(C) It enables the auditor to undertake remote

Downloaded from www.pdf.tube

Q. Audit with the computer
R. Audit through the computer
S. Manual techniques

List II: (Characteristic)

1. Uses a laptop as a terminal for remote on-line real time concurrent audit
2. Tests the logic and controls existing within the system directly
3. Involves Interviews, Questionnaires, and Control Flow Charts
4. Compares computer printouts with source documents ignoring internal logic

(A) P-4, Q-1, R-2, S-3
(B) P-1, Q-2, R-3, S-4
(C) P-4, Q-2, R-1, S-3
(D) P-2, Q-3, R-4, S-1

**May/June 2022**

**80.** Consider the following statements regarding the sourcing and development of computer auditors:

I Specialist computer auditors are often drawn from the EDP department.
II The computer manager would have the advantage of a qualified professional auditor on his staff.
III General training courses on computer auditing should be used.
IV Special qualifications in computer auditing, based on professional examinations, can be promoted.

Which of the above statements are correct?
(A) (I), (II), and (III)
(B) (II), (III), and (IV)
(C) (I), (III), and (IV)
(D) (I), (II), (III), and (IV)

**Oct/Nov 2023**

**81.** Three months after a new loan processing software goes live, the computer auditor conducts a review on a continuous basis to assure that all areas of the system are operating as intended. Which phase of the auditor's involvement does this represent?
(A) User Specifications phase
(B) System Test
(C) Post-implementation Review
(D) Implementation

**Oct/Nov 2010**

**82.** Which of the following best defines the "Audit with the computer" approach?
(A) Auditor laptop used as a terminal to audit apps on the server remotely
(B) Developing procedures to review manual inputs and printed output reports
(C) Testing the logic and controls existing within the application code directly
(D) Outsourcing the audit function entirely to a third-party vendor

**May/June 2005**

**83.** Which of the following is an exception to the disadvantages of the "Audit through the computer" approach?
(A) High costs are sometimes involved
(B) It requires extensive technical expertise when systems are complex
(C) It requires specialized competence on the part of the auditor
(D) It provides the auditor with increased power to effectively test a computer system

**Oct/Nov 2009**

**84.** Identify the correct statement regarding the User Specifications phase.
(A) It is the phase where the system analyst translates specs into IT concepts
(B) It involves conversion of technical specs into computer operating orders
(C) Basic functional concepts are defined by users and auditor defines controls
(D) It is an acceptance test conducted by the systems group and the user

NODIA

**May/June 2012**

**85.** The following question consists of two statements: Assertion (A) and Reason (R). Select the correct answer using the codes given below.
Assertion (A): The disadvantages of auditing through the computer, such as high costs and need for extensive technical expertise, are really spurious.
Reason (R): Auditing through the computer is often the only viable method of carrying out the audit in complex environments.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

on live applications. This scenario exemplifies which audit approach?
(A) Audit around the computer
(B) Audit with the computer
(C) Audit through the computer
(D) Manual techniques audit

**Oct/Nov 2017**

**73.** A financial institution processes millions of credit card transactions daily. The internal controls are deeply embedded in the application code, and there are substantial gaps in the visible audit trail. Which audit approach MUST the auditor use?
(A) Audit around the computer
(B) Manual technique audit
(C) Visual inspection of source documents
(D) Audit through the computer

**May/June 2008**

**74.** Consider the following statements about the competence of computer auditors:
I With the complexity of data processing, it is realistic to expect one person to have all the competence required to conduct all audits.
II Audit competence must be put together on a team basis.
Which of the above statements is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**Oct/Nov 2013**

**75.** The following question consists of two statements: Assertion (A) and Reason (R). Select the correct answer using the codes given below.
Assertion (A): The Implementation phase gives rise to the concept of "Conversion Audit".
Reason (R): The computer auditor should be concerned about the integrity and consistency of the data and procedures while porting from existing to the new system.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2015**

**76.** Consider the following principles of auditing around the computer:
I The auditor develops procedures to review input documents and output reports only.
II The auditor selects source documents to compare with computer printouts.
III It assumes that if input reflects properly in master files, processing functions are correct.
IV A review of computer programs or operations is deemed unnecessary.
V It requires extensive specialized technical training for the auditors.
Which of the above statements are correct?
(A) (I), (II), (III), and (IV)
(B) (I), (II), (IV), and (V)
(C) (II), (III), (IV), and (V)
(D) (I), (III), (IV), and (V)

**Oct/Nov 2012**

**77.** Identify the incorrect statement regarding the Detailed Technical Specifications & System Designing phase.
(A) The system analyst translates the user specifications into technical concepts
(B) This phase involves even closer coordination between the user and the EDP department
(C) The computer auditor reviews this phase to ascertain if a reasonable translation has been made with adequate security & control features
(D) All the programs and modules are tested here by programmers on an individual basis

**May/June 2011**

**78.** Conceptually, which of the following is a primary advantage of auditing through the computer?
(A) The auditor requires no technical expertise
(B) It is the simplest approach for small and simplistic software systems
(C) It avoids the need for reviewing computer programs
(D) Auditor can test a system effectively and ensure data is correct

**Oct/Nov 2020**

**79.** Match the computer audit approach (List-I) with its corresponding characteristic (List-II).
List I: (Computer Audit Approach)
P. Audit around the computer

Click Here to Buy book on Amazon

on-line real-time audits
(D) It requires extensive technical competence

May/June 2020

**66.** A bank is transitioning from a legacy software to a modern core banking system. The IS auditor is tasked with ensuring that all customer account balances from the old system match exactly with the balances populated in the newly deployed system. This specific activity aligns with which concept?
(A) Conversion Audit during Implementation
(B) Post-implementation Review
(C) System Planning
(D) General Audit Software stratification

Oct/Nov 2015

**67.** Consider the following examples of data items:
I Number of messages that have traversed each link
II Number of messages that have traversed each node
III Log of errors to identify locations and patterns of errors
IV Number of login attempts
Which of the above statements correctly identifies items kept in the operations audit trail?
(A) (I), (II), and (III)
(B) (II), (III), and (IV)
(C) (I), (II), and (IV)
(D) (I), (III), and (IV)

May/June 2013

**68.** Consider the following tools and certifications for an IT auditor:
I An IT auditor uses general tools and technical guides recommended by ISACA.
II Audit organizations encourage employees to obtain the CISA certification.
III CISA stands for Certified Information Systems Auditor.
IV CISA is awarded by ISACA.
V CISA certification ensures the auditor no longer needs team-based competence.
Which of the above statements are correct?
(A) (I), (II), (III), and (IV)
(B) (I), (II), (IV), and (V)
(C) (II), (III), (IV), and (V)
(D) (I), (III), (IV), and (V)

Oct/Nov 2021

**69.** Conceptually, why should the internal computer auditor be involved in the System Planning phase of SDLC?
(A) To anticipate developments and gain knowledge for new IT concepts
(B) To write the source code for the new application
(C) To define basic functional concepts from the end user's perspective
(D) To train the end users on the procedure manuals and instructions

May/June 2024

**70.** Identify the correct statement regarding "Audit through the computer".
(A) The approach assumes a review of operations is unnecessary
(B) It is tedious and comparisons are limited where data changes occur
(C) Auditor tests logic and controls within the system and its records
(D) It involves checking printouts against documents without knowing IT

Oct/Nov 2008

**71.** Match the SDLC phase (List-I) with its corresponding auditor activity (List-II).
List I: (SDLC Phase)
P. System Planning
Q. User Specifications
R. Programming
S. System Test
List II: (Auditor Activity)
1. Auditor defines controls by which the systems can be monitored
2. Auditor anticipates future system developments to gain necessary knowledge
3. Auditor verifies that tests are recorded and approvals are given before implementation
4. Auditor observes as technical specs are converted to source coding
(A) P-2, Q-1, R-4, S-3
(B) P-1, Q-2, R-3, S-4
(C) P-4, Q-3, R-2, S-1
(D) P-2, Q-4, R-1, S-3

NODIA

May/June 2006

**72.** An auditor connects their laptop as a terminal to the main server from a remote branch and uses their local software to run concurrent audits

Oct/Nov 2006

**86.** A bank's system processes complex interest calculations where input data goes through numerous changes and mathematical transformations before producing output reports. Why would an auditor avoid using the "Audit around the computer" approach in this scenario?
(A) Because specialized training is not needed
(B) True comparisons are limited when data undergoes frequent changes
(C) It provides comprehensive on-line real-time concurrent audit tools
(D) Because the visible audit trail is too substantial

May/June 2019

**87.** Which phase is considered the last line of defense before implementation, requiring tests to be recorded and test checks retained?
(A) System Planning
(B) System Test
(C) Programming
(D) Post-implementation Review

Oct/Nov 2022

**88.** Identify the incorrect statement regarding the circumstances where auditing through the computer must be used.
(A) The application system processes large volumes of input and produces large volumes of output
(B) The logic of the system is simple and processes small volumes of data manually
(C) Significant parts of the internal control system are embodied in the computer system
(D) Because of cost benefit considerations, there are substantial gaps in the visible audit trail

May/June 2018

**89.** Arrange the following critical phases of the Software Development Life Cycle (SDLC) in chronological order:
1. Detailed Technical Specifications & System Designing
2. User Specifications
3. System Planning
4. Programming

(A) 3, 2, 1, 4
(B) 2, 3, 1, 4
(C) 3, 1, 2, 4
(D) 1, 2, 3, 4

Oct/Nov 2016

**90.** Consider the following statements regarding the internal EDP audit department:
I It should conduct operational audits of data processing reviewing the computer centre.
II It should review the procedure for the development of new applications.
III It should review general controls over teleprocessing where this exists.
Which of the above statements are correct?
(A) (I) and (II)
(B) (I) and (III)
(C) (II) and (III)
(D) (I), (II), and (III)

NODIA

May/June 2014

**91.** A bank deployed an RPA chatbot to handle customer grievance tickets. However, due to faulty logic during setup, the bot routed all high-priority fraud reports to a low-priority generic inbox, alienating customers and delaying critical responses. This scenario exemplifies which specific RPA risk?
(A) Inherent bias
(B) Incorrect configuration
(C) Blockchain interoperability
(D) Quantum computing cyber-attacks

Oct/Nov 2007

**92.** Conceptually, what is the primary role of the Audit Committee of the Board concerning IS Audit findings?
(A) To personally execute the audit test procedures
(B) To write the source code for the bank's applications
(C) To review issues and provide guidance to management
(D) To design the Disaster Prevention and Recovery Plan

May/June 2025

**93.** Identify the incorrect statement regarding the common risks associated with RPA (Robotic Process Automation).
(A) Risks include inappropriate process selection and incorrect configuration
(B) An RPA system may incur unexpected costs if a bot replaces call centre staff but requires specialized maintenance

(C) RPA systems reduce complexity and do not necessitate any new safeguards regardless of data volume
(D) A chatbot designed to filter customer questions may delay passing customers to human contact due to incorrect configuration

**Oct/Nov 2019**

**94.** An IS Auditor is defining the scope of the audit for the upcoming financial year. They decide to use a methodology that assesses IT risks across the organization and defines the IS Audit Universe before execution. This scenario illustrates which critical process?
(A) Executing IS Audit
(B) Auditing around the computer for small systems
(C) Planning an IS Audit using Risk Based approach
(D) Program Code Comparison

**May/June 2009**

**95.** Identify the incorrect statement regarding emerging technologies.
(A) Operating through network nodes in blockchain exposes the organization to cyber-attacks and data hacks
(B) RPA is used to automate rarely repeated, highly complex strategic decision-making processes
(C) Both intentional and unintentional failures of AI must be considered by auditors
(D) The sheer volume of data passing through an RPA system may necessitate new safeguards and checks

**Oct/Nov 2011**

**96.** Match the Critical Components of IS Audit (List-I) with their corresponding descriptions (List-II).
List I: (Critical Components)
P. IS Audit
Q. Audit Charter
R. Planning
S. Reporting
List II: (Descriptions)
1. Involves aspects like IT risk assessment methodology and defining the IS Audit Universe
2. Involves preparing an audit summary memorandum for the CAE
3. Requires auditors to be independent, competent, and exercise due professional care
4. A document approved by the Board guiding the activities of the Internal Audit function
(A) P-3, Q-4, R-1, S-2
(B) P-4, Q-3, R-2, S-1
(C) P-1, Q-2, R-3, S-4
(D) P-2, Q-1, R-4, S-3

**May/June 2010**

**97.** Why must IS audit teams understand what emerging technologies will be used for, how they will be used, and by whom?
(A) Because they are responsible for coding Artificial Intelligence
(B) Because emerging technologies eliminate the need for Access Control
(C) Because Blockchain prevents any form of audit trail
(D) To assess new risks introduced and how management monitors them

**Oct/Nov 2024**

**98.** The Board of Directors of a bank mandates that the Internal Audit department must have a distinct subset of auditors specialized in evaluating IT controls, led by a dedicated head. According to standard banking regulatory guidelines, what is the specific name of this function?
(A) Information System Audit function
(B) General Audit Function
(C) External Audit Function
(D) Quality Assurance Function

**May/June 2017**

**99.** Which of the following is an exception to the critical components and processes of an IS Audit?
(A) Outsourcing relating to IS Audit
(B) Designing the bank's marketing campaigns
(C) Audit Charter / Audit Policy
(D) Planning an IS Audit

**Oct/Nov 2005**

**100.** Match the emerging technology (List-I) with its corresponding specific audit risk/challenge (List-II).
List I: (Emerging Technology)
P. Robotic Process Automation (RPA)
Q. Artificial Intelligence (AI)

Downloaded from www.pdf.tube

R. Blockchain
S. Big Data

List II: (Specific Audit Risk/Challenge)

1. Inherent bias from historical training data
2. Inability to reverse transactions and access data without required keys
3. Incorrect configuration causing delays in passing customers to a human contact
4. Used to inform audits but requires large data management (Data Analytics)

(A) P-3, Q-1, R-2, S-4
(B) P-1, Q-2, R-3, S-4
(C) P-2, Q-3, R-4, S-1
(D) P-3, Q-4, R-1, S-2

**May/June 2020**

**101.** Identify the correct statement regarding risk evaluation in IS Audit Outsourcing.
(A) Risk evaluation prior to agreement and periodic review
(B) Outsourcing automatically eliminates all IT risks for the bank
(C) Outsourced IS audits do not require an Audit Charter
(D) The Board is not responsible for outsourced audits

**Oct/Nov 2015**

**102.** What is the most appropriate risk consideration if a company's AI recruitment system is configured to make decisions based on historical hiring data?
(A) It reflects historical bias, shortlisting wrong candidates
(B) It will eliminate bias and ensure compliance with labor laws
(C) It will require interoperability with blockchain smart contracts
(D) It will require a significant increase in manual entry staff

**May/June 2013**

**103.** Match the Roles and Responsibilities (List-I) with their descriptions (List-II) in a banking environment.

List I: (Roles and Responsibilities)

P. Board of Directors and Senior Management
Q. Audit Committee of the Board
R. Internal Audit/IS Audit function
S. Chief Audit Executive (CAE)

List II: (Descriptions)

1. Devotes appropriate time to IS audit findings and provides guidance
2. Meets the responsibility to provide an independent audit function with sufficient resources
3. Assumes responsibility and accountability of the IS audit function
4. The entity to whom the IS Audit Head reports

(A) P-2, Q-1, R-3, S-4
(B) P-1, Q-2, R-4, S-3
(C) P-3, Q-4, R-1, S-2
(D) P-4, Q-3, R-2, S-1

**Oct/Nov 2021**

**104.** Which of the following is an exception to the issues an IS auditor should investigate regarding an AI system?
(A) Whether bias is identified, managed, and timely corrected
(B) How the AI system can be modified if external circumstances drastically change
(C) The physical risks if AI is used in products like autonomous vehicles
(D) The necessity of porting the AI system entirely to manual ledger accounting

**May/June 2024**

**105.** An IS Audit Head finalizes the test results and prepares a summary memorandum. They then present this document outlining critical IT security issues to the Audit Committee. Which critical component of the IS Audit process does this represent?
(A) Outsourcing relating to IS Audit
(B) System Test phase of SDLC
(C) Reporting and Follow up
(D) Implementing physical security

**Oct/Nov 2008**

**106.** Identify the correct statement regarding Emerging Trends in IS Audit.
(A) Technologies like RPA, AI, and Blockchain are well-established and no longer pose new risks
(B) Many IS audit teams are beginning to use Data Analytics and Big Data to inform their audits
(C) 5G and quantum computing are irrelevant to IS auditors
(D) Virtual reality and the internet of behaviours have replaced traditional financial auditing

NODIA

and losses
3. Ensuring the computer system achieves the goals of the organization and utilizes capacity well
4. Ensuring processing is uniform and not corrupted by manual intervention or virus

(A) P-2, Q-1, R-4, S-3
(B) P-1, Q-2, R-3, S-4
(C) P-4, Q-3, R-2, S-1
(D) P-3, Q-4, R-1, S-2

**May/June 2016**

**122.** Identify the incorrect statement regarding the Reporting and Follow up phase.
(A) This phase involves reporting audit findings to the CAE and Audit Committee
(B) The memorandum provides an overview of the entire audit processing from planning to audit findings
(C) An audit summary memorandum is prepared after the findings are presented to the Audit Committee
(D) It is an essential step to ensure findings are communicated to management

**Oct/Nov 2018**

**123.** Match the following audit concepts/tools (List-I) with their practical applications (List-II).
List I: (Audit Concepts/Tools)
P. Generalized Audit Software
Q. Integrated Test Facility (ITF)
R. Source Code Comparison
S. Passwords
List II: (Practical Applications)
1. Used as a logical security measure to restrict unauthorized access to the system
2. A concurrent audit technique to collect and evaluate evidences instantaneously
3. Analyzes data files, performs stratification, and extracts statistical samples
4. Identifies discrepancies between the audit version and the standard version of a program

(A) P-3, Q-2, R-4, S-1
(B) P-2, Q-3, R-1, S-4
(C) P-4, Q-1, R-2, S-3
(D) P-1, Q-4, R-3, S-2

**May/June 2007**

**124.** Which of the following is an exception to the elements that should be included in the Risk Based Audit Approach for IS Audit planning?
(A) Writing detailed technical specs for new software
(B) IT risk assessment and management methodology
(C) Defining the IS Audit Universe
(D) Scoping and planning the audit

**Oct/Nov 2014**

**125.** The following question consists of two statements: Assertion (A) and Reason (R). Select the correct answer using the codes given below.
Assertion (A): The internal computer auditor needs to be involved in the critical phases of the Software Development Life Cycle (SDLC).
Reason (R): Early involvement allows the auditor to define controls, review potential exposures, and ensure a reasonable translation of user specifications into technical concepts.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

www.nodia.in

Click Here to Buy book on Amazon

(B) Organizations using blockchain are exempt from anti-money-laundering legislation
(C) Auditors ensure management monitors the evolving legal landscape
(D) Blockchain eliminates the need for internal IS audit teams

**Oct/Nov 2020**

**114.** What is the most appropriate action required from IS Auditors before reporting findings to the CAE and Audit Committee?
(A) Delete the audit trail to maintain confidentiality
(B) Prepare a summary memorandum providing an audit overview
(C) Fire the IT staff responsible for the errors
(D) Purchase a new core banking system

**May/June 2022**

**115.** A bank enters into a contract with a third-party vendor to conduct its IS Audit. Prior to finalizing the agreement, the bank evaluates the risks associated with this arrangement. This process is a requirement under which critical component of information system auditing?
(A) Executing IS Audit
(B) Audit Committee of the Board
(C) Audit around the computer
(D) Outsourcing relating to IS Audit

**Oct/Nov 2023**

**116.** Which of the following is an exception to the risks associated with AI (Artificial Intelligence)?
(A) The system creating more entry points and connections, increasing potential risks
(B) Inherent bias resulting from AI systems being primed with data collected over a long period
(C) Physical risks if a company uses AI in autonomous vehicles or heavy machinery maintenance
(D) The inability to reverse transactions and access data without required keys

**Oct/Nov 2010**

**117.** During a review of the database systems, an auditor extracts data, runs analytical tests using CAATTs, and documents the findings of unauthorized access. This activity best represents which stage of the IS Audit process?
(A) Reporting and Follow up
(B) Planning an IS Audit
(C) Board of Directors approval
(D) Executing IS Audit

**May/June 2005**

**118.** Conceptually, why is interoperability essential for blockchain in an organizational context?
(A) It allows the blockchain to be easily hacked
(B) It ensures that the system can be audited without a computer
(C) It replaces the need for an Audit Committee
(D) It must communicate with external systems to function properly

NODIA

**Oct/Nov 2009**

**119.** Identify the incorrect statement regarding the planning and execution phases of an IS Audit.
(A) Executing IS Audit is entirely outsourced to the Board of Directors without auditor involvement
(B) Banks need to carry out IS Audit planning using the Risk Based Audit Approach
(C) During execution, auditors should obtain evidences and perform test procedures
(D) The planning phase involves aspects like IT risk assessment methodology and defining the IS Audit Universe

**May/June 2023**

**120.** What is the most appropriate risk stemming from an organization's blockchain transactions with unknown external organisations?
(A) Exposure to anti-money-laundering legislation violations
(B) Increased efficiency in efficiency auditing
(C) Reduction in the physical security requirements of the System Room
(D) Unauthorized alteration of the operating system source code

**Oct/Nov 2025**

**121.** Match the basic objectives of System Audit (List-I) with their implications (List-II).
List I: (Basic Objectives)
P. Safeguarding Assets
Q. Maintaining Data Integrity
R. Maintaining Process Integrity
S. System Efficiency & Effectiveness
List II: (Implications)
1. Ensuring data is complete, accurate, without distortion, and appears as desired
2. Protecting hardware, software, human ware, and physical manuals from damages

May/June 2006

**107.** The following question consists of two statements: Assertion (A) and Reason (R). Select the correct answer using the codes given below.
Assertion (A): Because the IS Audit is an integral part of the Internal Auditors, auditors will also be required to be independent, competent, and exercise due professional care.
Reason (R): IS Auditors are exempt from professional standards since they focus on IT rather than financial statements.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

Oct/Nov 2017

**108.** A tech firm utilizes AI to predict equipment failure in its factories. However, due to a sudden shift in global supply chains, the historical data parameters became irrelevant, and the AI failed to predict critical breakdowns. This highlights the audit need to inquire about:
(A) How to modify the AI if external circumstances change
(B) How to implement a Dead Man's Door in the factory
(C) How to restrict concurrent user connections for the AI
(D) The physical security of the blockchain nodes

May/June 2008

**109.** Identify the correct statement regarding the Audit Charter / Audit Policy.
(A) It is an informal verbal agreement between the CAE and the IT manager
(B) It explicitly excludes IS Audit from financial auditing
(C) It prevents the use of Risk Based Audit Approaches
(D) Board approval and annual review for continued relevance

Oct/Nov 2013

**110.** The following question consists of two statements: Assertion (A) and Reason (R). Select the correct answer using the codes given below.
Assertion (A): Management of an RPA system may pose a risk if used to automate an area where frequent changes are implemented.
Reason (R): It may necessitate additional layers of processes each time a change occurs, which adds time and complexity.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2015

**111.** Conceptually, which of the following best describes the "IS Audit Universe"?
(A) The physical location of bank servers and hardware
(B) The external vendors providing cloud services
(C) The biometric data of all bank employees
(D) The set of IT areas and processes subject to IS Audit

Oct/Nov 2012

**112.** The following question consists of two statements: Assertion (A) and Reason (R). Select the correct answer using the codes given below.
Assertion (A): Organizations using blockchain must follow specific protocols and management processes to avoid being locked out and have clear contingency plans.
Reason (R): Blockchain's strengths, such as the inability to reverse transactions and access data without required keys, can also be its weaknesses.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2011

**113.** Identify the correct statement regarding regulatory compliance and blockchain.
(A) The regulatory landscape for blockchain is fixed and developed

Downloaded from www.pdf.tube

# ANSWERS

1. (D) It ensures IT systems are protected, reliable, and properly managed
System Audit ensures IT infrastructure remains resilient and properly managed. It focuses on protecting technological assets and verifying data integrity. This process mitigates risks associated with computerized environments, providing assurance that systems are reliable for business operations. By evaluating controls, auditors help maintain organizational stability and compliance within complex information systems, ultimately safeguarding interests.

2. (C) Object Code Comparison
Object Code Comparison is a technique used to verify the authenticity of software versions. It involves comparing the object code of the program currently in use with an authorized audit version. This method ensures that no unauthorized changes or modifications have been made to the production code, thereby confirming that the software performing business processes is legitimate.

3. (C) The cost must not be greater than the benefits arising out of it
Maintaining data integrity requires balancing the cost of controls against the potential benefits. An organization should not spend more on ensuring data accuracy and completeness than the value gained or the loss prevented. This economic principle ensures that resources are allocated efficiently while minimizing financial risks associated with distorted, incomplete, or inaccurate information within the system.

4. (C) Both (I) and (II)
Audit software provides significant advantages by operating independently of the systems being examined. It typically utilizes read-only copies of data files to ensure the original organizational information remains untouched and uncorrupted during the sampling process. These characteristics allow auditors to perform thorough evaluations without compromising the integrity of live databases or interfering with daily operations.

5. (A) (I) and (II)
Generalized Audit Software empowers auditors to access and analyze data directly from various computerized media. It incorporates essential functions like arithmetic calculations, stratification, and frequency analysis to evaluate data quality. Unlike specialized tools, it focuses on examining data records rather than checking program source codes for unauthorized changes, making it a versatile instrument for broad data evaluation.

6. (A) (I), (II), (III), and (IV)
Environmental controls are vital for protecting the physical infrastructure where computer systems operate. These include power management tools like UPS systems and stabilizers to ensure uninterrupted supply. Additionally, fire detection, temperature regulation, and moisture control protect hardware from physical damage. Measures like pest control further safeguard equipment, though logical security like passwords falls under a different control category.

7. (B) An audit of the computer system
System Audit specifically refers to the comprehensive examination and evaluation of a computer system. This process reviews the hardware, software, and related controls to ensure assets are protected and data remains integrated. It goes beyond simple financial auditing by focusing on the technological framework, operational efficiency, and the overall effectiveness of the information technology infrastructure within an organization.

8. (B) Program Code Comparison - Compares program codes of the audit version with the standard version
Program Code Comparison involves a systematic review of the coding between different software versions. By comparing the audit-verified code with the version currently in use, auditors can identify unauthorized modifications or deviations. This technique is essential for ensuring that only approved logic is executed within the system,

NODIA

where the internal transformation of data is minimal.

**77.** (D) All the programs and modules are tested here by programmers on an individual basis
During the detailed technical specifications phase, analysts translate user requirements into IT concepts, requiring close coordination between users and the EDP department. The auditor reviews this to ensure security and control features are properly integrated. Testing individual programs and modules, however, is primarily a part of the programming or unit testing phase rather than the initial design and specification translation.

**78.** (D) Auditor can test a system effectively and ensure data is correct
A primary advantage of auditing through the computer is the auditor's ability to effectively test the internal logic of a system. By examining the code and embedded controls, the auditor gains a higher level of assurance that data is processed correctly. This approach is essential for complex environments where a visible audit trail may be missing or insufficient for manual verification.

**79.** (A) P-4, Q-1, R-2, S-3
Different audit approaches have distinct characteristics. Auditing around the computer compares printouts to source documents. Auditing with the computer uses tools like laptops for remote, real-time testing. Auditing through the computer directly examines the system's internal logic and controls. Finally, manual techniques involve using interviews and questionnaires to evaluate the control environment and procedures without relying on automated tools.

**80.** (D) (I), (II), and (III), and (IV)
Organizations develop computer auditors by drawing specialists from EDP departments and utilizing professional training courses. Promoting specialized qualifications, such as those offered through professional examinations, further enhances the department's capabilities. This multifaceted approach ensures that the audit function possesses both the technical depth and the professional auditing rigor needed to evaluate complex and evolving information technology environments effectively.

**81.** (C) Post-implementation Review
A post-implementation review is conducted after a system has been operational for a certain period. Its purpose is to evaluate whether the software is functioning as intended and meeting its objectives on a continuous basis. This phase allows auditors to identify any operational issues or control weaknesses that may only become apparent once the system is used in a live environment.

**82.** (A) Auditor laptop used as a terminal to audit apps on the server remotely
The audit with the computer approach utilizes technology to perform auditing tasks more efficiently. This often involves the auditor using their own hardware, like a laptop, as a terminal to remotely access and audit applications on a main server. By leveraging these tools, auditors can conduct concurrent tests and analyze data without being physically present at the server's primary location.

**83.** (D) It provides the auditor with increased power to effectively test a computer system
Auditing through the computer often involves high costs and requires significant technical expertise to evaluate complex system logic. While these are considered disadvantages, this approach provides the auditor with increased power to effectively test a computer system. This increased capability is a major benefit rather than a drawback, as it allows for a more thorough and reliable examination of internal controls.

**84.** (C) Basic functional concepts are defined by users and auditor defines controls
In the user specifications phase, the basic functional concepts of a new system are defined from the perspective of the end-users. During this time, the computer auditor also defines the controls necessary to monitor the system effectively. This ensures that business needs are met while maintaining security and accountability before any technical coding or system design begins in later phases.

**85.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Some argue that the disadvantages of auditing through the computer, such as cost and

Click Here to Buy book on Amazon

# STUDYING FROM PDFs?

# THINK AGAIN.

If you are studying only from PDFs,
you are wasting valuable time.

Research shows that learning from

**PRINTED BOOKS** has up to

**4× HIGHER RETENTION**

than studying from screens.

**PRINT BOOK = BETTER MEMORY**

**PDF = LOWER RETENTION**

Those who study from **PRINTED BOOKS**
move **AHEAD.**

Others are left **BEHIND**
in competition.

In competitive exams,
being average is not enough.

## STAY ONE STEP AHEAD.

17. (A) Multi-layer security is more effective than a single barrier in networking
Implementing multiple layers of security provides a defense-in-depth strategy that is significantly more effective than a single barrier. If one control fails, subsequent layers continue to protect the network and data from threats. This approach complicates unauthorized access attempts and ensures that vulnerabilities at one level do not lead to a complete compromise of the entire computer architecture and systems.

18. (A) Only (I)
Internal auditors possess a deep understanding of organizational procedures and systems, allowing them to perform thorough reviews. However, their proximity to management can sometimes lead to influence or a lack of perceived independence. In contrast, external auditors provide an impartial perspective but often require more time to grasp the specific nuances and complexities of the organization's unique internal IT systems.

19. (D) Designing the physical IT infrastructure
Computer-Assisted Audit Techniques (CAATs) are primarily used for audit-related activities such as evaluating the accuracy and completeness of data, performing analytical reviews, and verifying records with real-world entities. These functions support auditors in ensuring data reliability and integrity. However, designing physical IT infrastructure belongs to system development and engineering, not auditing, and therefore is not a function of CAATs.

20. (C) Assertion (A) is true, but Reason (R) is false.
Program Source Code Review is an effective method for identifying erroneous, unauthorized, or non-standard code within a system. However, Generalized Audit Software is primarily intended for analyzing data files and evaluating data quality rather than directly examining program codes. Therefore, while the assertion regarding source code review is correct, the reason describing the primary purpose of GAS is inaccurate.

21. (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
A Dead Man's Door system utilizes a dual-door entry mechanism to prevent unauthorized individuals from following authorized personnel into restricted areas. The first door must fully close and lock before the second door opens, ensuring only one person is in the buffer zone at a time. This physical control effectively eliminates the risk of piggybacking and enhances overall facility security.

22. (B) Setting organizational macroeconomic policies
Information technology audits typically cover areas such as system development, physical environment, and user application access. They focus on the controls and risks associated with the computer systems and data. However, setting organizational macroeconomic policies falls under the jurisdiction of senior management and economic planners rather than being a standard component of an IT audit's operational or technical scope.

23. (D) Reject the system as the implementation cost exceeds the resulting benefits
In system auditing, control implementations should be guided by cost-benefit analysis. If the cost of an encryption solution exceeds the financial benefits gained from preventing data distortion, the system should generally be rejected. Allocating resources to a project where expenditures significantly outweigh the potential risk mitigation is not considered economically sound or logical for an organization seeking efficient operations.

24. (D) Depreciation of the office real estate
Auditors use various parameters to measure system effectiveness, such as task accomplishment, technical efficiency, and organizational impact. These metrics help determine if the IT system is achieving its intended goals. However, the depreciation of office real estate is a general accounting concern and does not serve as a qualitative or quantitative parameter for evaluating the performance of a computer system.

25. (B) Concurrent Arithmetic and Analytical Test Tools
Concurrent audit techniques include the Integrated Test Facility, System Control Audit Review File, and Continuous and Intermittent Simulation. These methods allow for real-time monitoring and evidence collection during system

Downloaded from www.pdf.tube

accurately attributed to one specific terminal and individual session.

**43.** (B) Maker-Checker
The maker-checker concept is a fundamental control involving the segregation of duties. It requires one person to initiate a transaction and another to authorize it before processing. This ensures that no single individual has total control over a financial activity, reducing the risk of errors and fraud. It is a practical application of maintaining accountability within core banking applications.

**44.** (A) Only (I)
Processing controls are designed to ensure that systems handle data correctly and maintain the integrity of application programs. They verify that the logic within the software remains uncorrupted and functions as intended. While auditors may compare computer-generated results with manual derivations, the primary definition of these controls focuses on ensuring accurate processing by protecting the internal logic of the systems.

**45.** (C) Number of retransmissions occurring across each network link
An accounting audit trail for communication subsystems typically includes message sequence numbers, dispatch times, and source identifiers. These items help reconstruct message flows. However, the number of retransmissions occurring on a specific network link is generally categorized as operations audit trail data. Operations data focuses on network performance and error patterns rather than the specific accounting and accountability of messages.

**46.** (B) 10 years
Password security significantly increases with length due to exponential growth in possible combinations. A tool that cracks a four-character password in seconds would require a drastically longer time for an eight-character password. For a standard set of characters, this jump can increase the cracking time from mere seconds to approximately ten years, demonstrating why longer passwords provide much stronger logical protection.

**47.** (B) The operations audit trail maintains a record of attempted or actual resource consumption within a system
The operations audit trail records the consumption of system resources and monitors overall performance. Unlike the accounting audit trail, which tracks the source and nature of data updates for accountability, the operations trail focuses on system health and resource usage. It provides valuable information to administrators regarding attempted or actual usage of hardware and software components within the computerized environment.

**48.** (B) Ensuring that the data entering the system is correct and error-free
Output controls aim to prevent unauthorized alterations, delivery to incorrect persons, and the willful suppression of reports. They ensure that information generated by the system is handled securely. However, ensuring that data entering the system is correct and error-free is the primary objective of input controls rather than output controls. Output controls focus on the final distribution and storage phases.

NODIA

**49.** (A) Controls of Last Resort
Controls of Last Resort include measures taken to mitigate the financial impact of catastrophic risks that cannot be entirely prevented. Insuring physical IT assets against natural disasters like earthquakes is a prime example. This ensures the organization can recover costs and replace hardware if a disaster occurs. These controls provide a final safety net for organizational resilience when primary preventions fail.

**50.** (A) (I), (II), and (III)
Database controls are essential for data resilience and include making regular backups to magnetic tapes or other media. These backups should be stored at off-site locations to protect against site-wide disasters. Occasional restoration tests are necessary to ensure the tapes remain functional. Contrary to some assumptions, antivirus packages remain necessary to protect the database from corruption even when backups exist.

**51.** (C) Both (I) and (II)
Database system audit trails provide a time series of events recording user attempts to access system resources. This allows management and auditors

**34.** (D) Identity of users, authentication info, and login attempt counts
An accounting audit trail at the database system level maintains specific data items for security and accountability. This includes the unique identity of users, their authentication information, and a record of login attempt counts. These logs allow auditors to reconstruct events and verify who accessed or attempted to access system resources, ensuring that all actions can be traced to individuals.

**35.** (A) Maker-Checker - One person enters data and checks it themselves
To ensure adequate input controls, organizations should implement a maker-checker system where one person enters data and another verifies it. Overlapping roles should be avoided to maintain segregation of duties. Additionally, input forms must have authorized signatures and be validated to prevent fraudulent entries. Allowing the same person to enter and check data is a significant control failure.

**36.** (A) To identify network problems and reconfigure the network accordingly
Network supervisors utilize operations audit trail data to monitor system performance and health. By reviewing logs of message transit times and queue lengths, they can identify bottlenecks or technical problems within the network. This information allows for timely reconfiguration and optimization of the infrastructure, ensuring that the communication subsystem remains efficient and reliable for all organizational users.

**37.** (A) Dead Man's Door (Deadman doors)
A Dead Man's Door is a physical security mechanism designed to prevent unauthorized entry through piggybacking. It consists of two doors where the first must close and lock before the second can be opened. This ensures that only one person enters the restricted area at a time, effectively stopping unauthorized individuals from following authorized employees into sensitive server or system rooms.

**38.** (A) (I), (II), (III), and (IV)
Output preservation is maintained through systematic procedures that ensure reports reach authorized personnel and are stored securely. Checked outputs should be returned to designated officials and filed centrally in proper sequence. Maintaining these records for their required retention period is crucial. However, careless handling of reports after the retention period expires should never be encouraged, as data must be destroyed.

**39.** (D) A chronological record of system events to answer queries and fulfill laws
An audit trail is a chronological record of system events that tracks data from its source to its final destination. It serves to answer queries, fulfill legal requirements, and provide a history of user activities. By maintaining a detailed log of transactions and access attempts, organizations can ensure accountability, detect unauthorized actions, and verify the integrity of their information systems.

**40.** (D) Applying specific security codes for restricted menu access
In a menu-driven application, restricted menus can be protected by applying specific security codes or access rights. This ensures that only authorized users with the correct credentials can view or utilize sensitive functions. Such logical controls are essential for preventing unauthorized individuals from accessing critical administrative or financial features that could compromise the integrity and security of the entire software package.

**41.** (A) (I) and (II)
The accounting audit trail for a communication subsystem records specific details about message movement. This includes the unique identifiers of every node traversed and the exact time and date each node was reached. These data items allow auditors to track the path and timing of communications, ensuring accountability and facilitating the reconstruction of message flows in case of disputes.

**42.** (C) Preventing users from logging in on more than one computer at a single time
Restriction to concurrent connections is a logical security control that prevents a single user ID from being logged into multiple computers simultaneously. By limiting access to one active session at a time, the system reduces the risk of account sharing and unauthorized access. This feature ensures that user activities can be

Click Here to Buy book on Amazon

thereby maintaining the security and reliability of the application software.

**9.** (B) Audit software corrupts the organization's data by using a write-enabled copy of the file during sampling
Auditors use specialized software to analyze organizational data without risking its integrity. This software is designed to use read-only or duplicated files for sampling and analysis purposes. Any claim that audit software intentionally or naturally corrupts live data by using write-enabled copies is factually incorrect, as a primary goal of auditing is to preserve data accuracy.

**10.** (A) 2, 3, 1, 4, 5, 6
The logical sequence of an information systems audit begins with establishing objectives and scope. Following this, auditors develop a strategic plan and gather information regarding relevant IT controls. They then perform specific tests using CAATs to evaluate system performance. Finally, findings are reported to management, followed by a necessary follow-up phase to ensure corrective actions are taken.

**11.** (D) UPS systems, voltage stabilizers, and redundant power infrastructure
To prevent data corruption from utility grid fluctuations, organizations must implement robust power-related environmental controls. Mechanisms such as Uninterruptible Power Supply systems and voltage stabilizers are critical for maintaining a steady electrical flow. Redundant power infrastructure further ensures that sudden spikes or outages do not damage hardware or cause the loss of vital digital information during processing.

**12.** (C) Efficiency auditing evaluates user characteristics before a system has been running
Efficiency auditing evaluates how well a system utilizes resources and whether productivity has improved after implementation. It typically examines hardware adequacy and user characteristics while the system is operational. It is incorrect to suggest that efficiency auditing evaluates user characteristics before the system has been running, as the focus is on performance during actual system usage and execution.

**13.** (A) Any computer program utilized to improve the audit process, like data software
Computer Aided Audit Tools and Techniques encompass various software programs designed to enhance the efficiency and effectiveness of the auditing process. These tools allow auditors to perform data extraction, analysis, and validation across complex digital environments. They automate repetitive tasks and enable the examination of large datasets that would be impossible to review through traditional manual audit methods.

**14.** (C) (I), (II), and (IV)
Computer Aided Audit Tools and Techniques involve diverse software applications, including data extraction utilities and business intelligence programs like Crystal Reports. These tools help auditors perform complex data analysis efficiently. While databases like MS Access are also included in this category, physical security devices and manual checklists are excluded. They provide a technological approach to improving the overall audit process.

**15.** (D) (I), (II), (III), and (IV)
A computerized environment requires a variety of controls to ensure operational integrity and security. Access controls manage user permissions, while input controls verify the accuracy of data entry. Communication controls protect data during transmission, and database controls safeguard stored information. Together, these elements form a comprehensive framework that protects the system from errors, unauthorized access, and potential data loss.

**16.** (A) Maximizing marketing efficiency
System Audit focuses on four primary objectives: safeguarding technological assets, maintaining data integrity, ensuring process integrity, and achieving organizational effectiveness and efficiency. While these goals support business success, maximizing marketing efficiency is not considered a core objective of an information systems audit. The audit's focus remains on the security, reliability, and performance of the underlying IT infrastructure and data.

NODIA

to reconstruct activities and verify compliance. Periodic analysis of these trails is necessary to identify potential control weaknesses or unauthorized access patterns. Both documenting activities and analyzing them are critical for maintaining the overall security and integrity of databases.

**52.** (D) Terminal restriction limits a user to working on one specific machine only
Logical security includes terminal restriction, which limits a specific user's access to a designated machine. This ensures that even with valid credentials, an individual cannot log in from unauthorized locations. Other features like removing dormant users and keeping activity logs are equally important. However, keeping user IDs of transferred staff active or granting all users operating system rights compromises security.

**53.** (C) Database Controls - Uses backups to maintain data integrity
Database controls play a vital role in maintaining the integrity and availability of stored data. The use of regular backups ensures that information can be recovered in the event of corruption or hardware failure. This specific pairing is correct because it directly addresses the protection and restoration of data assets, which is a core function of effective database management systems.

**54.** (C) Accounting audit trail and Operations audit trail
Every robust information system must maintain two primary types of audit trails: the accounting audit trail and the operations audit trail. The accounting trail tracks the source and movement of data for accountability purposes. The operations trail records resource consumption and system performance events. Together, they provide a complete history of what occurred within the system and how resources were utilized.

**55.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Disaster Prevention and Recovery Plans are essential for business continuity and should incorporate risk assessment and impact analysis. These plans identify potential disasters and establish methods to prevent them or minimize their consequences. By preparing for various scenarios, organizations can protect their IT infrastructure and ensure that critical operations can be restored quickly following an unexpected and damaging event.

**56.** (A) At least 8 characters with upper/lower cases, numbers, and special symbols
Robust logical security requires passwords that are difficult to crack through brute force or guessing. A standard requirement includes a minimum length of eight characters, combining upper and lower case letters, numbers, and special symbols. This complexity significantly increases the time needed for automated tools to compromise credentials, thereby providing a stronger layer of protection for user accounts and systems.

**57.** (A) Public network owners always supply required audit trail information
Communication audit trails trace messages through network nodes from dispatch to receipt. This information is vital if messages are lost or disputes arise. However, it is incorrect to assume that public network owners always supply all required audit trail data. Organizations must often implement their own tracking mechanisms to ensure they have the necessary details for auditing their specific communications.

**58.** (A) P-2, Q-4, R-1, S-3
Password security features involve several mechanisms to protect system access. Password expiry dates compel periodic credential changes, while grace logins allow limited access after expiration. Unique password rules prevent the reuse of old credentials, and minimum length requirements ensure complexity. Each of these features works together to strengthen logical security and reduce the likelihood of unauthorized users gaining access to accounts.

**59.** (A) P-4, Q-1, R-3, S-2
Security controls are categorized by their specific functions. Access controls use biometrics and passwords to manage entries. Output controls protect reports from careless handling. Environmental controls, such as pest and water damage control, safeguard the physical surroundings of the system. Finally, Controls

Downloaded from www.pdf.tube

operations. There is no standard recognized technique referred specifically as Concurrent Arithmetic and Analytical Test Tools within the established framework of automated auditing, making this pair inaccurate in professional contexts.

**26.** (D) It ensures uniform, uncorrupted computer system processing
Maintaining process integrity ensures that computer systems execute operations in a uniform and uncorrupted manner. This objective focuses on preventing unauthorized manual interventions or virus-induced changes during processing. By ensuring that software performs exactly as intended without any erratic behavior, the organization can rely on the consistency and reliability of its automated business functions and overall technological operations.

**27.** (B) (I) and (III)
Security and control measures are primarily implemented to prevent the loss of valuable data and costly computer resources. They also aim to stop incorrect decisions resulting from fraudulent or inaccurate information. While testing might involve simulated errors, the overall goal is not to encourage errors but to ensure the reliability, accuracy, and safety of the organization's information system environment.

**28.** (A) P-3, Q-4, R-1, S-2
The planning process for a system audit involves specific chronological steps. It begins by reviewing the latest audit reports to take necessary preliminary actions. Next, auditors obtain and document an understanding of the system being audited. They then determine the most efficient audit strategy to be employed. Finally, the planned audit strategy is documented to guide the entire execution phase.

**29.** (C) It uses dummy data to test if a program contains specific processing errors
The test data approach involves using dummy information to verify the processing logic of a computer program. By feeding specific data into the system, auditors can observe if the software handles errors and transactions correctly. This method helps identify potential flaws in the program's internal controls and processing functions without requiring the extraction of live transaction data from master files.

**30.** (A) (I), (II), (III), and (IV)
Generalized Audit Software performs various critical tasks by combining functional capabilities. It evaluates data quality, examines the existence of entities, and analyzes system processing. Additionally, it facilitates analytical reviews through stratification and statistical sampling. However, its primary focus is on data and software logic rather than examining the physical hardware architecture of database servers, which requires different inspection methods.

**31.** (C) Maker-Checker allows the same person entering data to perform the final check
Input controls are designed to prevent the entry of inaccurate or fraudulent data into a system. A key principle is the maker-checker concept, which requires two different individuals: one to enter the data and another to verify it. It is incorrect to allow the same person to perform both tasks, as this bypasses segregation of duties and increases risk.

NODIA

**32.** (B) Off-site storage of backups under database controls
Off-site storage of database backups is a critical control for disaster recovery. By keeping copies of data in a geographically separate location, an organization ensures that information can be restored even if the primary server room is destroyed. This scenario demonstrates how effective database controls and remote backup facilities provide resilience against severe physical disasters like fires or structural damage.

**33.** (B) The allowed logins for a user after their password has officially expired
Grace login is a security feature that allows a user to access the system for a limited number of times after their password has officially expired. This mechanism ensures that employees are not immediately locked out of their accounts during critical tasks while still compelling them to update their credentials promptly to maintain the logical security standards of the organization.

**68.** (A) (I), (II), (III), and (IV)
IT auditors often utilize tools and technical guides provided by organizations like ISACA. Professional certifications, such as the Certified Information Systems Auditor (CISA), are highly encouraged to validate expertise. While these qualifications demonstrate high individual competence, they do not eliminate the need for team-based auditing in complex environments. Successful IS audits still rely on the combined skills of diverse professionals.

**69.** (A) To anticipate developments and gain knowledge for new IT concepts
Internal computer auditors should be involved in the system planning phase to anticipate future developments and gain early knowledge of new IT concepts. This proactive involvement allows them to provide input on control requirements and prepare for future auditing needs. It ensures that security considerations are integrated into the project from its inception rather than being added as an afterthought.

**70.** (C) Auditor tests logic and controls within the system and its records
Auditing through the computer involves a direct examination of the logic and controls residing within the system's software and records. This approach allows the auditor to verify that the internal processing functions correctly handle transactions. Unlike auditing around the computer, this method requires technical expertise to evaluate the effectiveness of embedded controls and ensures that the system's output is reliable.

**71.** (A) P-2, Q-1, R-4, S-3
Different SDLC phases involve specific auditor activities. In system planning, the auditor anticipates developments to gain knowledge. During user specifications, they define controls for monitoring. The programming phase involves observing the conversion of technical specs into code. Finally, in the system test phase, the auditor verifies that all tests are recorded and proper approvals are granted before implementation occurs.

**72.** (B) Audit with the computer
Auditing with the computer involves using technology as a tool to conduct the audit process. A common example is an auditor using a laptop as a terminal to connect to a server and perform concurrent, real-time tests on live applications. this approach leverages the computer's processing power to enhance the auditor's ability to collect and evaluate evidence from remote locations.

**73.** (D) Audit through the computer
When a system processes vast volumes of transactions with controls embedded deep in the code and lacks a visible audit trail, auditors must use the through the computer approach. This method allows them to test internal logic and controls directly. Relying on manual techniques or auditing around the computer would be insufficient for verifying the accuracy of such complex processing.

**74.** (B) Only (II)
Due to the extreme complexity of modern data processing, it is unrealistic to expect a single individual to possess all the specialized skills required for every audit. Therefore, audit competence must be established on a team basis. Combining different areas of expertise ensures a comprehensive evaluation of systems, from technical infrastructure to financial logic and organizational procedural controls.

**75.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
The implementation phase of the software development life cycle introduces the concept of a conversion audit. This is necessary because the computer auditor must ensure the integrity and consistency of data as it is ported from old systems to new ones. Verifying that procedures and information remain accurate during this transition is critical for maintaining overall organizational data quality and reliability.

**76.** (A) (I), (II), (III), and (IV)
Auditing around the computer is based on the principle that if input documents match output reports, the internal processing is assumed correct. The auditor develops procedures to review these visible records without examining the internal software logic or programs. This approach does not require extensive technical training, making it accessible for simpler systems

Click Here to Buy book on Amazon

of Last Resort, like Disaster Prevention and Recovery Plans, provide a strategy for survival after catastrophic failures occur.

**60.** (A) (I) and (II)
In mainframe environments, security is often managed through the operating system and its utilities. In distributed processing systems, communication security relies heavily on the Network Operating System. While technology has advanced, networking has actually increased the risk of message interception rather than decreasing it. Therefore, managing communication controls remains a complex and critical task for maintaining overall information system security.

**61.** (C) Audit around the computer, Audit through the computer, Audit with the computer
The three fundamental approaches to computer auditing are auditing around the computer, auditing through the computer, and auditing with the computer. Each method offers a different level of technical involvement, ranging from simple input-output comparisons to direct testing of internal system logic and using the computer as a tool to perform concurrent audits on live organizational data and processing.

**62.** (A) Audit competence being put together on a professional team basis
Auditing complex technological systems requires a specialized skill set that traditional auditors may lack. To address this, organizations often form professional teams that combine financial expertise with deep IT knowledge, sometimes by recruiting specialists from EDP departments. This collaborative approach ensures that the audit team has the necessary competence to effectively evaluate complicated software and underlying technical control environments.

**63.** (C) Assertion (A) is true, but Reason (R) is false.
Auditing around the computer is a simple, familiar approach where auditors compare input documents with output reports without examining internal system logic. While this method is considered easy to use for simple systems, it does not involve a direct review of the internal processing functions. Therefore, the reason provided for its simplicity—that the auditor examines internal logic—is factually incorrect.

**64.** (C) Creating source coding and translating technical specifications
During the user procedures and training phase, organizations prepare manuals for system operation and conversion. This ensures that staff can effectively use and transition to the new application. However, creating source coding and translating technical specifications are activities associated with the programming and design phases rather than user procedure development. Training focuses on the human application and operation of systems.

**65.** (A) It is tedious and comparisons are limited as input data changes
A major disadvantage of auditing around the computer is that it is tedious and provides limited results when data undergoes frequent changes. Because the auditor only compares inputs and outputs, they lack insight into how the system transforms data. This approach fails to provide high confidence in the accuracy of internal processing when transactions are complex or high in volume.

**66.** (A) Conversion Audit during Implementation
A conversion audit is performed during the implementation phase of a new system. It focuses on ensuring that data ported from the legacy system to the new software remains consistent, complete, and accurate. Verifying that customer account balances match exactly between systems is a critical part of this process, safeguarding the integrity of financial information during the transition to new technology.

**67.** (A) (I), (II), and (III)
The operations audit trail focuses on system performance and resource management. It records data such as the number of messages traversing links and nodes, as well as logs of errors to identify patterns. These items help network supervisors monitor the health of the subsystem. Information regarding the number of login attempts, however, is typically categorized as an accounting or security audit trail item.

NODIA

complexity, are spurious because it is often the only viable method for complex systems. When a visible audit trail is absent or processing is highly intricate, direct testing of internal logic becomes essential. The necessity of the approach in modern IT environments justifies the resource investment required.

**86.** (B) True comparisons are limited when data undergoes frequent changes
Auditing around the computer is unsuitable for systems where data undergoes numerous mathematical transformations or changes. In such cases, comparing simple inputs to outputs does not provide enough information to verify the accuracy of the complex internal processing. Therefore, the auditor cannot gain sufficient confidence in the system's logic, making a more technical through the computer approach necessary.

**87.** (B) System Test
The system test phase is the final line of defense before a new application is implemented. It requires that all tests be meticulously recorded and that test checks be retained for future reference. This phase ensures that the system operates correctly under various conditions and that all necessary approvals have been secured before the software moves into the production environment.

**88.** (B) The logic of the system is simple and processes small volumes of data manually
Auditing through the computer is mandatory when significant controls are embedded in the software or when the audit trail is missing due to cost-benefit gaps. It is also required for systems handling large data volumes. However, if a system has simple logic and processes small amounts of data manually, auditing through the computer is typically not necessary, as simpler methods suffice.

**89.** (A) 3, 2, 1, 4
The development of software follows a logical chronological sequence. It starts with system planning, where the project's foundation is laid. Next, user specifications are defined to outline functional needs. These are then translated into detailed technical specifications and system designs. Finally, the programming phase begins, where technical specifications are converted into actual source code for the new application.

**90.** (D) (I), (II), and (III)
An internal EDP audit department has broad responsibilities, including conducting operational audits of the data centre and reviewing procedures for developing new applications. They also evaluate general controls over teleprocessing and communication systems. By performing these diverse reviews, the department ensures that all aspects of the organization's information technology infrastructure are secure, efficient, and aligned with management's control objectives.

**91.** (B) Incorrect configuration
Incorrect configuration is a significant risk in Robotic Process Automation. In this scenario, a chatbot's faulty setup caused critical fraud reports to be misrouted, leading to delays and customer dissatisfaction. This demonstrates how human error during the initial programming or configuration phase of an RPA bot can result in operational failures and unintended negative consequences for the organization's processes.

**92.** (C) To review issues and provide guidance to management
The Audit Committee of the Board plays a supervisory role by reviewing IS audit findings and providing guidance to management. They do not perform the tests or write code themselves. Instead, they devote time to understanding critical IT issues and ensuring that management takes appropriate steps to address identified weaknesses, thereby maintaining the organization's overall governance and risk management framework.

NODIA

**93.** (C) RPA systems reduce complexity and do not necessitate any new safeguards regardless of data volume
Robotic Process Automation introduces risks like inappropriate process selection and configuration errors. While bots handle high volumes of repetitive tasks, their implementation does not reduce system complexity. In fact, the sheer volume of data they process often necessitates new safeguards and checks. Claiming that RPA eliminates the need for additional safeguards

(C) Agreement between bodies within the same organization - Internal SLA
(D) Agreement guarding against expectation creep for an external provider - Internal SLA

**May/June 2020**

**30.** Which of the following statements regarding the evaluation of proposals is incorrect?
(A) Proposal openings are open to the public and are scheduled two to four weeks after the pre-proposal conference.
(B) A prerequisite for award is that the vendor must submit a responsive offer that conforms in all material respects to the RFP.
(C) When all proposals are determined to be non-responsive, all must be rejected and a new RFP issued.
(D) Proposals received after the last date of submission are marked with the time and date received and included in the bid process.

**Oct/Nov 2019**

**31.** During which step of the SLA Negotiation phase is the actual agreement reached, requiring key members of both parties to review the document and offer suggestions for improvement?
(A) Step 1.1 Assess whether an SLA is appropriate
(B) Step 2.5 Determine a plan for monitoring
(C) Step 3.2 Finalize SLA
(D) Step 3.1 Create a draft SLA

**May/June 2009**

**32.** Which of the following is a recognized sound Change Management process?
(A) Applying patches immediately without an inventorying strategy to save time and resources.
(B) Ensuring application changes are managed using configuration management processes and a baseline.
(C) Proceeding with application updates without a defined roll-back methodology to minimize SLA size.
(D) Ignoring the root cause of an incident if the system restores automatically during the cycle.

**Oct/Nov 2007**

**33.** Read the following Assertion (A) and Reason (R) and choose the correct option:
Assertion (A): The SLA process should be rolled-out initially in a selected area where SLAs are needed the most.
Reason (R): If the SLA is the wrong solution, it may waste time, result in a loss of resources, and damage the relationship between the parties.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2011**

**34.** According to data center architecture architecture principles, why might an architect consciously choose not to correct every single identified SPOF?
(A) Because removing a SPOF always invalidates the existing SLA.
(B) Because modern servers automatically eliminate all hardware components as a SPOF.
(C) Because cross-site clustering is technically impossible for legacy banking applications.
(D) Because in some cases, the cost to correct a SPOF is costlier than the benefits of the workloads at risk.

**Oct/Nov 2010**

**35.** Consider the following activities performed by IT staff during a phased application portfolio assessment:
I Identifying potential issues.
II Conducting interviews with appropriate IT resources.
III Identifying applications that can easily be outsourced.
IV Bypassing baseline reporting to accelerate the project.
Which combination of statements is correct?
(A) (I), (II), and (III)
(B) (II), (III), and (IV)
(C) (I), (III), and (IV)
(D) (I), (II), and (IV)

**May/June 2024**

**36.** Consider the following components of an integrated stack defined as a "workload" in data center management:

Downloaded from www.pdf.tube

**102.** (A) It reflects historical bias, shortlisting wrong candidates
AI systems used for recruitment can inadvertently reflect historical biases present in the training data they consume. If previous hiring practices were biased, the AI may continue shortlisting candidates based on those same flawed parameters. Auditors must consider this risk to ensure the system does not perpetuate unfairness or lead to the selection of the wrong candidates for the organization.

**103.** (A) P-2, Q-1, R-3, S-4
In a bank, senior management provides an independent audit function with adequate resources. The Audit Committee reviews findings and provides guidance. The Chief Audit Executive assumes accountability for the IS audit function and reports to the Audit Committee. The IS audit head also has a reporting line to the CAE. Each role is critical for ensuring effective governance and technological security.

**104.** (D) The necessity of porting the AI system entirely to manual ledger accounting
When auditing AI, investigators should check for bias management and how the system adapts to external changes. Physical risks, particularly in autonomous systems, are also critical. However, suggesting that an AI system should be ported entirely to manual ledger accounting is illogical and an exception to standard audit investigations, as it contradicts the primary purpose of implementing automated AI solutions.

**105.** (C) Reporting and Follow up
The reporting and follow-up phase is where the IS audit head finalizes test results and prepares a summary memorandum. This document outlines critical IT security issues for the Audit Committee's review. This stage is vital for communicating findings to senior leadership and ensuring that management understands the identified risks and takes necessary actions to remediate vulnerabilities within the information system.

**106.** (B) Many IS audit teams are beginning to use Data Analytics and Big Data to inform their audits
Emerging trends in IS auditing involve the increasing use of data analytics and big data to inform the audit process. These technologies allow auditors to examine larger datasets and identify patterns that traditional methods might miss. As technological landscapes evolve with tools like AI and RPA, audit teams must adapt their techniques to effectively evaluate the risks associated with these advancements.

**107.** (C) Assertion (A) is true, but Reason (R) is false.
IS auditors are part of the internal audit function and must adhere to professional standards of independence, competence, and due professional care. Their focus on IT does not exempt them from these requirements. Professional auditing rigor is essential for providing reliable assurance on the security and integrity of information systems, regardless of whether the audit is technical or financial in nature.

**108.** (A) How to modify the AI if external circumstances change
When AI systems rely on historical data that becomes irrelevant due to shifting external circumstances, they may fail to make accurate predictions. This highlights the critical audit need to inquire about the system's flexibility and how it can be modified or updated when global parameters change. Ensuring that AI remains relevant is essential for maintaining operational reliability in dynamic environments.

**109.** (D) Board approval and annual review for continued relevance
An audit charter or policy is a formal document that requires approval from the Board of Directors. It establishes the authority and responsibilities of the internal audit function, including IS audit. The charter must be reviewed annually to ensure it remains relevant to the organization's needs and regulatory requirements, providing a solid foundation for conducting risk-based audit approaches.

**110.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Using RPA in areas subject to frequent changes can increase operational risk. Each change may require the creation of additional process layers for the bots, adding time and complexity to the system. This can lead to inefficiencies or errors if the bots are not updated correctly, demonstrating why management must carefully select and

NODIA

regardless of data volume is incorrect and compromises organizational security.

**94.** (C) Planning an IS Audit using Risk Based approach
Planning an information systems audit using a risk-based approach involves assessing IT risks across the organization. This process includes defining the IS audit universe, which identifies all areas and processes subject to evaluation. By focusing on the highest-risk areas first, auditors can allocate resources effectively and ensure that the most critical components of the technological infrastructure are thoroughly examined.

**95.** (B) RPA is used to automate rarely repeated, highly complex strategic decision-making processes
RPA is typically used to automate repetitive, rules-based tasks rather than highly complex, strategic decision-making processes. Strategic decisions usually require human judgment that bots cannot replicate. Emerging technology risks include cyber-attacks on blockchain nodes and potential failures in AI. Auditors must evaluate how these technologies are used and ensure that management implements appropriate monitoring and failure-prevention safeguards across the organization.

**96.** (A) P-3, Q-4, R-1, S-2
IS auditing involves several critical components. The audit process itself requires independent, competent auditors. An audit charter, approved by the Board, guides the internal audit function's activities. Planning involves risk assessment and defining the audit universe. Reporting requires preparing a summary memorandum for the Chief Audit Executive. Together, these elements ensure a structured and professional approach to evaluating information systems.

**97.** (D) To assess new risks introduced and how management monitors them
Auditors must understand the purpose and users of emerging technologies to assess the new risks they introduce. This knowledge allows them to evaluate how management monitors these technologies and whether existing safeguards are sufficient. As technologies like AI and blockchain change the organizational landscape, auditors need this understanding to ensure that the audit process remains relevant and effectively addresses vulnerabilities.

**98.** (A) Information System Audit function
In the banking sector, regulatory guidelines mandate the establishment of a specialized function dedicated to evaluating IT controls. This is known as the information system audit function. It is a distinct subset of the internal audit department, led by a dedicated head, and focuses specifically on the security, reliability, and integrity of the technological infrastructure and related digital business processes.

**99.** (B) Designing the bank's marketing campaigns
The scope of IS auditing includes creating an audit charter, planning based on risk, and managing outsourcing relationships related to the audit function. These activities ensure that IT controls are effectively evaluated. However, designing marketing campaigns is a business operational function unrelated to the critical components of information system auditing, which focuses on security, data integrity, and process reliability within technology.

**100.** (A) P-3, Q-1, R-2, S-4
Emerging technologies present unique risks. RPA may suffer from incorrect configurations that delay customer service. AI can exhibit inherent bias derived from its training data. Blockchain faces challenges related to transaction irreversibility and the necessity of secure keys. Big data requires robust management and analytics to inform the audit process. Each technology demands specific auditing strategies to address these distinct vulnerabilities.

**101.** (A) Risk evaluation prior to agreement and periodic review
When an organization outsources its IS audit function, it must perform a thorough risk evaluation before finalizing any agreement. Following this, periodic reviews are necessary to ensure the service provider continues to meet standards. Outsourcing does not eliminate IT risks or the Board's ultimate responsibility, and the outsourced function must still operate within the framework of an established audit charter.

Click Here to Buy book on Amazon

**119.** (A) Executing IS Audit is entirely outsourced to the Board of Directors without auditor involvement

IS audit execution requires auditors to gather evidence and perform tests, while planning involves risk assessment and defining the audit universe. It is incorrect to claim that the entire execution of an IS audit is outsourced to the Board of Directors. The Board's role is oversight and providing guidance, while the actual audit tasks are carried out by professional IS auditors.

**120.** (A) Exposure to anti-money-laundering legislation violations

Transacting with unknown external organizations via blockchain exposes a company to significant risks, including potential violations of anti-money-laundering legislation. Because blockchain can facilitate anonymous or pseudonymous transfers, management must implement robust monitoring and due diligence procedures. IS auditors evaluate these controls to ensure the organization is not inadvertently facilitating illegal activities or breaching international financial regulations through decentralized technology.

**121.** (A) P-2, Q-1, R-4, S-3

System audit objectives carry specific implications for organizational security. Safeguarding assets protects hardware and software from damage. Maintaining data integrity ensures information is accurate and complete. Maintaining process integrity keeps system execution uniform and uncorrupted. Finally, system efficiency and effectiveness focus on achieving organizational goals and optimizing resource usage. Each objective is essential for a reliable and secure IT environment.

**122.** (C) An audit summary memorandum is prepared after the findings are presented to the Audit Committee

The reporting and follow-up phase involves communicating audit findings to the Chief Audit Executive and the Audit Committee through a summary memorandum. This document provides an overview of the audit process and results. It is incorrect to state that the memorandum is prepared only after findings are presented, as it serves as the primary tool for that presentation and communication.

**123.** (A) P-3, Q-2, R-4, S-1

Audit tools have diverse applications in computerized environments. Generalized Audit Software is used for analyzing data files and statistical sampling. The Integrated Test Facility allows for concurrent testing of live systems. Source code comparison helps identify unauthorized modifications by checking different program versions. Passwords serve as a fundamental logical security measure, restricting access to authorized users and protecting sensitive system functions.

**124.** (A) Writing detailed technical specs for new software

Planning an IS audit using a risk-based approach includes IT risk assessment, defining the audit universe, and scoping the audit. These steps ensure that the evaluation focuses on the most critical areas. However, writing detailed technical specifications for new software is a development task performed by system analysts, not a component of the planning process for an information systems audit.

**125.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).

Internal computer auditors must be involved in critical SDLC phases to define controls and review potential exposures early. This proactive approach ensures that user specifications are reasonably translated into technical concepts with adequate security. Early involvement allows for the integration of control requirements during design, which is more effective and less costly than attempting to fix security issues after implementation.

NODIA
www.nodia.in

monitor the processes automated through robotic systems.

**111.** (D) The set of IT areas and processes subject to IS Audit
The IS audit universe is a conceptual term representing the complete set of IT areas, processes, and systems within an organization that are subject to auditing. It defines the boundaries of what the IS audit function will evaluate. Establishing this universe is a critical step in the planning phase, as it allows auditors to assess risks and prioritize their evaluation activities.

**112.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Blockchain's fundamental features, such as transaction irreversibility and the need for specific keys, are both its greatest strengths and potential weaknesses. If keys are lost or errors occur, the data may become inaccessible or permanent. Therefore, organizations must follow strict protocols and management processes, including clear contingency plans, to avoid being locked out of their own critical information and systems.

**113.** (C) Auditors ensure management monitors the evolving legal landscape
As the regulatory environment for blockchain continues to evolve, auditors must ensure that management actively monitors the legal landscape. Organizations using blockchain are not exempt from existing laws, such as anti-money-laundering legislation. IS auditors play a key role in verifying that the organization's use of this technology remains compliant with all relevant local and international regulations and legal requirements.

**114.** (B) Prepare a summary memorandum providing an audit overview
Before reporting findings to the Chief Audit Executive and the Audit Committee, IS auditors must prepare a comprehensive summary memorandum. This document provides an overview of the entire audit process, from planning to the final test results. It serves as a concise summary that allows senior leadership to quickly understand the most critical security issues and management concerns identified during evaluation.

**115.** (D) Outsourcing relating to IS Audit
Outsourcing IS audit activities requires a structured approach to risk management. Before finalizing a contract with a third-party vendor, the organization must evaluate the potential risks associated with the arrangement. This process is a mandatory component of managing outsourced audit functions, ensuring that the external provider can deliver high-quality, independent evaluations while meeting the organization's specific security and regulatory needs.

**116.** (D) The inability to reverse transactions and access data without required keys
Artificial Intelligence presents risks such as inherent bias, increased entry points for attacks, and physical dangers in autonomous applications. However, the inability to reverse transactions and access data without required keys is a characteristic specific to blockchain technology rather than a standard risk associated with AI. Auditors must distinguish between these technological features to correctly assess the vulnerabilities of each system.

**117.** (D) Executing IS Audit
The execution phase of an IS audit involves performing actual test procedures and gathering evidence. This includes extracting data from databases, running analytical tests with CAATTs, and documenting instances of unauthorized access. This hands-on activity allows the auditor to verify the effectiveness of controls and identify specific security failures within the live environment, leading to the development of audit findings.

**118.** (D) It must communicate with external systems to function properly
For blockchain to function effectively within an organizational context, it must be able to communicate with external systems. This interoperability allows for the seamless transfer of information and value across different platforms. Without the ability to interact with other technologies and databases, a blockchain remains isolated, which limits its utility and prevents it from being properly integrated into business processes.

Downloaded from www.pdf.tube

exactly what it wants or does not know what is available in the marketplace?
(A) Request for Proposal
(B) Request for Information
(C) Request for Bid
(D) Service Level Agreement

**May/June 2008**

**8.** Why is it critical that deliverables be explicitly and well defined in the cost proposal format of an RFP?
(A) To prevent vendors from submitting information regarding their internal financial capacities.
(B) To facilitate a comparative analysis of costs by ensuring all vendors respond to the same deliverables.
(C) To ensure that the mandatory pre-proposal conference can be skipped by all participating vendors.
(D) To automatically eliminate vendors who rely on single-source purchasing methodologies for service.

**Oct/Nov 2011**

**9.** Given below are two statements regarding Internal SLAs:
Statement I: An internal SLA is typically less rigorous than an external SLA because renegotiating is not usually an option when internal customers need more.
Statement II: Internal service providers can apply the exact same types of remedies and financial incentives internally as external providers do.
Which of the above statement(s) is/are correct?
(A) Only Statement I
(B) Only Statement II
(C) Both Statement I and Statement II
(D) Neither Statement I nor Statement II

**May/June 2022**

**10.** During a pre-proposal conference for a new custodial services contract, a vendor asks a technical question regarding the scope of work. A representative from the organization verbally clarifies the requirement, which materially affects the existing bid document. What is the contractual standing of this oral clarification?
(A) It becomes immediately binding on all participating vendors.
(B) It is binding only on the vendor who raised the question.
(C) It cannot be relied upon unless it is documented in a written addendum to the bid document.
(D) It forces the immediate cancellation of the current bid document and the issuance of a new one.

**Oct/Nov 2017**

**11.** When analyzing the financial impact of an adequate SLA, how does spending more resources (money and time) during the setup and contract stages affect the later phases?
(A) It permanently increases the maintenance costs throughout the operations phase.
(B) It delays the transition-out phase indefinitely.
(C) It equates to a financial loss identical to the initial high spending area.
(D) It results in substantial financial gains for the client in the operations and exit phases.

**May/June 2014**

**12.** Which two stages of a contractual relationship require intense focus in order to ensure the smoothness of the subsequent operations and transition-out stages?
(A) Contract and Transition-in
(B) Evaluation and Setup
(C) Setup and Contract
(D) Operations and Contract

**Oct/Nov 2005**

**13.** Following the award of a contract for desktop maintenance, the vendor repeatedly fails to meet the agreed-upon repair timelines. The project coordinator issues a notice demanding a corrective action plan within a specified time period. Under which specific contractual provision is this action typically cited?
(A) The standard default clause
(B) The single-source purchase clause
(C) The expectation creep provision
(D) The contract negotiation addendum

**May/June 2019**

**14.** Read the following Assertion (A) and Reason (R) and choose the correct option:
Assertion (A): An evaluation matrix is prepared to assist individuals responsible for evaluating proposals.
Reason (R): The evaluation matrix allows

NODIA

organizations to bypass the sealed competitive bid procedure by directly scoring vendors on unlisted technical criteria.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2012**

**15.** In a typical CBS environment, the vendor is expected to maintain specific disaster recovery metrics. What does Recovery Time Objective (RTO) signify?

(A) A measure of data that may be allowed to be lost in case of a disaster.
(B) The maximum CPU utilization limit allowed during user access time.
(C) The timeline required to finalize the negotiation phase of the SLA.
(D) The time taken to resume operations in case of a disaster.

**May/June 2005**

**16.** Which document is explicitly utilized when an organization knows precisely what it needs and has formulated precise requirements and specifications?

(A) Request for Bid
(B) Request for Information
(C) Request for Proposal
(D) Service Level Agreement

**Oct/Nov 2024**

**17.** A commercial bank has an external SLA with a vendor for ATM cash replenishment. For three consecutive months, the vendor fails to meet the guaranteed service levels, causing significant customer dissatisfaction. Depending on the terms of the contract, what are the possible actions the bank may take?

(A) Terminate the contract, renegotiate terms, or continue with the existing arrangement.
(B) Initiate a legal suit against the internal compliance department while starting a new RFB process.
(C) Immediately convert the external SLA into an internal SLA without modifying any existing metrics.
(D) Bypass the contract change management log and adjust the system RPO to zero without notice.

**May/June 2021**

**18.** Alpha Bank is planning to upgrade its legacy Core Banking System. The management has a broad understanding of the functional requirements but expects the vendors to propose customized, complex solutions that may vary significantly in approach. Which solicitation methodology should the Purchasing Office adopt to initiate this procurement?

(A) Develop and publish a Request for Proposal to evaluate multiple potential solutions.
(B) Float a Request for Bid to get the lowest pricing for the upgrade.
(C) Issue a Request for Information to assess the precise specifications required.
(D) Proceed directly to Contract Co-ordination to negotiate terms with a known vendor.

**Oct/Nov 2016**

**19.** What is the primary objective of implementing a Service Level Agreement (SLA) in an outsourcing engagement?

(A) To eliminate the need for an RFP during the competitive bid process.
(B) To legally protect the service provider from all financial liabilities during operational disruptions.
(C) To ensure that the vendor assumes ownership of the internal business processes.
(D) To establish and manage expectations of customers, reducing confusion while defining acceptable service.

**May/June 2012**

**20.** Consider the following statements regarding the prerequisites for an award:

I The vendor must possess the requisite business integrity.
II The vendor must possess the financial and organizational capacities to ensure good-faith performance.
III The vendor must conform in all material respects to the RFP to be considered responsive.

Which combination of statements is correct?

(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only

Click Here to Buy book on Amazon

(D) (I), (II), and (III)

**Oct/Nov 2020**

**21.** For optimum response to users, which typical utilization threshold for Memory or CPU usage during user access time is often stipulated in an SLA?
(A) 50%
(B) 90%
(C) 70%
(D) 100%

**May/June 2007**

**22.** Which of the following statements correctly differentiates the types of solicitation documents used by the Purchasing Office?
(A) An RFB is used for complex projects with potential for multiple solutions, whereas an RFP requires precise specifications.
(B) The information received from an RFI may assist in determining whether a formal request for bid or proposal is necessary.
(C) An RFP is utilized when an organization lacks any general idea of its requirements and seeks market availability.
(D) An RFI requires mandatory pre-proposal meetings for vendors to attend.

**Oct/Nov 2018**

**23.** What is the primary operational objective of conducting a pre-proposal conference during the RFP process?
(A) To negotiate the final pricing terms with the shortlisted vendors.
(B) To determine the bid limit for the expected contract performance.
(C) To finalize the internal Service Level Agreement between the departments.
(D) To ensure all vendors receive the same information and receive constructive feedback about the RFP.

**May/June 2016**

**24.** Consider the following basic objectives of an internal SLA:
I To boost productivity.
II To increase employee morale.
III To enable one department to legally sue another within the organization.
IV To assist in the development of business processes.
Which combination of statements is correct?
(A) (I), (II), and (III)
(B) (I), (III), and (IV)
(C) (I), (II), and (IV)
(D) (II), (III), and (IV)

**Oct/Nov 2009**

**25.** Under what specific condition is negotiation normally permitted by the Purchasing Office after the receipt of proposals?
(A) When all proposals are determined to be completely non-responsive.
(B) Only where effective competition is not available and if mentioned in the RFP document.
(C) When the vendors fail to attend the mandatory pre-proposal meeting.
(D) When the cost proposals exceed the predetermined internal budget limits.

**May/June 2025**

**26.** What is the correct chronological sequence of the four major stages in the life cycle of a contractual relationship?
(A) Setup, Contract, Transition-in, Operations
(B) Setup, Contract, Operations, Transition-out
(C) Requirements, Setup, Contract, Operations
(D) Requirements, Evaluation, Setup, Contract

**Oct/Nov 2022**

**27.** Which phenomenon describes a situation where one party's assumptions of another become higher than what may be considered reasonable, a risk that an SLA specifically guards against?
(A) Expectation creep
(B) Scope specification
(C) Vendor compliance
(D) Operational phase out

**May/June 2018**

**28.** In the context of the RFP process, what document acts as the yardstick against which the vendor's performance is measured?
(A) The Statement of Work
(B) The evaluation matrix
(C) The Service Level Agreement
(D) The contract change management log

**Oct/Nov 2013**

**29.** Which of the following pairs correctly represents the distinction in SLA types?
(A) Local Partner Agreement - External SLA
(B) Legally binding contract between two organizations - Internal SLA

Downloaded from www.pdf.tube

# CHAPTER 19

# Competitive Bid Process: RFP and SLA

**Oct/Nov 2014**

**1.** Consider the following statements regarding the necessity of a formal RFP:
Statement I: A formal RFP is always required for justified single-source purchases.
Statement II: An RFP is needed when the product or services required exceed a certain bid limit and the terms cannot be completely described by a detailed specification.
Which of the above statement(s) is/are correct?
(A) Only Statement I
(B) Only Statement II
(C) Both Statement I and Statement II
(D) Neither Statement I nor Statement II

**May/June 2023**

**2.** Match the following major domains of outsourcing in a CBS Environment in List I with their contextual scope in List II:
List I: (Outsourcing Domains)
P. SOC
Q. DWH
R. Help Desk
S. Peripherals
List II: (Scope)
1. Data Ware House
2. Security Operations Centre
3. Call Centre operations
4. Hardware at Branches
(A) P-2, Q-1, R-3, S-4
(B) P-1, Q-2, R-4, S-3
(C) P-3, Q-4, R-1, S-2
(D) P-4, Q-3, R-2, S-1

**Oct/Nov 2006**

**3.** What is defined as a hybrid document used when an organization has a general idea with some specifications or is handling a large, complex project with potential for multiple solutions?
(A) Request for Information
(B) Request for Bid
(C) Request for Proposal
(D) Service Level Agreement

NODIA

**May/June 2010**

**4.** Read the following Assertion (A) and Reason (R) and choose the correct option:
Assertion (A): By applying a well-defined and orderly approach when setting up SLAs, outsourcing vendors are able to provide measurable and enforceable results.
Reason (R): SLAs provide requisite methodologies for root cause analysis of problems, leading to easier, faster fixes and lower overall risk.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2021**

**5.** Which of the following is NOT typically listed as one of the essential contents to be included in an RFP document?
(A) Task description
(B) Source code of the existing legacy applications
(C) Contractor personnel requirements
(D) Organization responsibilities

**May/June 2015**

**6.** During a disaster recovery audit, the auditor checks the Recovery Point Objective (RPO) defined in the SLA for the bank's Core Banking System. What should be the ideal expected value for the RPO in this critical environment?
(A) Between 2 to 6 hours
(B) Zero and near-zero
(C) Equal to the RTO limit
(D) Exactly 70% of utilization

**Oct/Nov 2025**

**7.** Which of the following solicitation documents is used when an organization does not know

I Application and Middleware.
II Database.
III Operating system.
Which of the above component(s) is/are included in this stack?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

**Oct/Nov 2008**

**37.** The basic sequence of steps of the SLA process includes all of the following phases EXCEPT:
(A) Liquidation
(B) Commitment
(C) Preparation
(D) Management

**May/June 2006**

**38.** Consider the following statements regarding the 'Conventions' section under the 'General Clauses' of an SLA:
I Detail the definitions of time used in the SLA.
II Define the dates and key words used in the document.
III Outline the rewards and financial remedies for vendor non-compliance.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

**Oct/Nov 2015**

**39.** What is the precise definition of "System Resiliency" in the context of data center architecture?
(A) The inherent inability of a legacy system to operate under heavy workloads without degradation.
(B) The process of bypassing fault-tolerant technology during planned outages.
(C) The methodology of scheduling critical workloads exclusively within a public cloud environment.
(D) A facility architecture feature enabling uninterrupted service delivery despite component failures.

**May/June 2013**

**40.** Consider the following steps involved in the Management phase of the SLA process:
I Report attained service levels.
II Monitor service levels by reviewing reports.
III Periodically review the SLA to reflect changes in technology and customer requirements.
Which of the above statement(s) is/are correct?
(A) (I) and (II) only
(B) (I) and (III) only
(C) (II) and (III) only
(D) (I), (II), and (III)

**Oct/Nov 2023**

**41.** When a workload is described as "platform independent," what does it technically imply?
(A) It can only run on legacy physical mainframes.
(B) It can run in physical, virtual, or cloud computing environments.
(C) It does not require an operating system to function.
(D) It is immune to single points of failure without clustering.

**May/June 2017**

**42.** Match the steps of the SLA Preparation phase in List I with their corresponding objectives in List II:
List I: (SLA Preparation Steps)
P. Assess current services
Q. Determine working configuration and environment
R. Gather customer feedback
S. Determine a plan for monitoring services
List II: (Objectives)
1. Provide a baseline to assess customer satisfaction after SLA implementation.
2. Draft Key Performance Indicators (KPIs) by both parties.
3. Verify whether the environment has an impact on the service provision.
4. Determine realistic service levels that can be provided before making commitments.
(A) P-4, Q-3, R-1, S-2
(B) P-1, Q-2, R-4, S-3
(C) P-3, Q-1, R-2, S-4
(D) P-4, Q-1, R-3, S-2

Click Here to Buy book on Amazon

(C) 25 times more
(D) 50 times more

**Oct/Nov 2014**

**85.** Consider the following elements that can be leveraged to address service level challenges:
I Named executives and management participants.
II Defined and measurable commitments.
III Escalation procedures.
IV Regular and scheduled communication.
Which combination of statements is correct?
(A) (I), (II), and (III)
(B) (II), (III), and (IV)
(C) (I), (III), and (IV)
(D) (I), (II), (III), and (IV)

**May/June 2023**

**86.** Which of the following sets of tools should be deployed to analyze the I/O performance of a bank's servers?
(A) GFI LanGuard and Open NMS
(B) VTune Performance Analyzer and Iometer
(C) Fiddler and Nagios Network Analyzer
(D) Wireshark and Packet Tracer

**Oct/Nov 2006**

**87.** Read the following Assertion (A) and Reason (R) and choose the correct option:
Assertion (A): Outsourcing provides a bank with increased time availability for management to focus on key management functions.
Reason (R): The benefits of outsourcing include efficiencies in operations, increased ability to acquire current technology, and shorter lead time in delivering services to customers.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2010**

**88.** Why is it important for a performance monitoring solution to allow the specification of both an upper and lower-level range for alerts, rather than just an upper-level threshold?
(A) To track user login attempts during off-peak hours only.
(B) Because network latency can only be measured from a lower-level bound.
(C) Because metrics like voltage or temperature cause failures if they fall outside a specific range.
(D) To measure the purely financial impact of adequate SLA deployment throughout the project.

**Oct/Nov 2021**

**89.** According to recent surveys on SLAs, organizations that implement the best SLA and Vendor Management practices comprise what percentage of total organizations?
(A) 5%
(B) 10%
(C) 20%
(D) 50%

**May/June 2015**

**90.** Which statement about the established reporting process in SLA implementation is incorrect?
(A) There should be an established reporting format and a regular process to review it.
(B) The process should identify where SLAs are not met.
(C) Improvements regarding unmet SLAs should be reported back to a steering committee.
(D) The process must hide the reasons for unmet SLAs from the steering committee to preserve vendor relations.

**Oct/Nov 2025**

**91.** According to regulatory guidelines, when outsourcing to a provider outside the home country, the bank must ensure the arrangement does not hinder which of the following, EXCEPT:
(A) The ability of the bank or regulatory authorities to perform periodic audits/ inspections.
(B) The vendor's ability to maximize their operational profits.
(C) The ability of the regulator to reconstruct activities of the bank based on books and records.
(D) The timely access to necessary documentation by supervising bodies.

**May/June 2008**

**92.** Consider the following characteristics of a well-written scope of work in an RFP:

NODIA

(B) An emergency hardware replacement of the database servers.
(C) A Request for Information to the patch developer.
(D) An immediate renegotiation of the SLA parameters.

**May/June 2008**

**50.** Which of the following elements is incorrectly paired with its SLA subgroup?
(A) Scope — General Clauses
(B) Service Description — Services and Service Levels
(C) Rewards and Remedies — General Clauses
(D) Escalation Procedures — Management Elements

**Oct/Nov 2011**

**51.** Match the scheduler goals in List I with their definitions in List II:
List I: (Scheduler Goals)
P. Maximizing throughput
Q. Minimizing response time
R. Minimizing latency
S. Maximizing fairness
List II: (Definitions)
1. Equal CPU time to each process according to priority.
2. Time from work becoming enabled until the first point it begins execution.
3. Total amount of work completed per time unit.
4. Time between work becoming enabled and its subsequent completion.
(A) P-3, Q-2, R-4, S-1
(B) P-4, Q-1, R-2, S-3
(C) P-2, Q-3, R-1, S-4
(D) P-3, Q-4, R-2, S-1

**May/June 2022**

**52.** Two parties are entering an outsourcing agreement but possess conflicting opinions about the use of SLAs. To allow the terms to be tested and revised early, the vendor proposes using an SLA Template. According to the standard SLA Negotiation phase, which two resources should be consulted alongside the template to aid the drafting process?
(A) Request for Bid and RTO metrics
(B) Vendor Performance Matrix and Setup Manual
(C) Internal Customer Feedback and Financial Impact Graph
(D) SLA Catalogue and SLA Guidance Material

**Oct/Nov 2017**

**53.** In the detailed SLA Process flow for a Trilateral agreement, who is typically involved alongside the Organization and the Data Originator?
(A) The Third-party Auditor
(B) The Competitor
(C) The Regulator
(D) The Hardware Vendor

**May/June 2014**

**54.** Match the concepts related to system architecture in List I with their corresponding operational realities in List II:
List I: (Architecture Concepts)
P. Fault tolerance
Q. Single Point of Failure (SPOF)
R. Server clustering
S. Redundant switches
List II: (Operational Realities)
1. Prevents catastrophic failure from logic errors or component failing.
2. Allows a duplicate copy of an application to run on a second physical server if the first fails.
3. Provides alternative paths for interconnected servers to avoid a network disconnect.
4. Can compromise the availability of workloads or the entire data center if triggered.
(A) P-1, Q-4, R-2, S-3
(B) P-2, Q-3, R-1, S-4
(C) P-4, Q-1, R-3, S-2
(D) P-3, Q-2, R-4, S-1

**Oct/Nov 2005**

**55.** Match the components of the SLA Structure in List I with their descriptions in List II:
List I: (SLA Components)
P. Scope
Q. Term
R. Conventions
S. Parties to the Agreement
List II: (Descriptions)
1. Details definitions of time, dates, and other key words.
2. Describes and names the legal entities and responsible persons.
3. Agrees upon the quality and quantity of delivered services and customer business

Downloaded from www.pdf.tube

Q. Evaluates proposals against criteria
R. Agrees on the awarded firm
S. Monitors the contractor's performance post-award

List II: (Entities/Actions)
1. Department monitors
2. Purchasing Office
3. Department and/or committee members
4. Purchasing department

(A) P-2, Q-3, R-4, S-1
(B) P-4, Q-1, R-2, S-3
(C) P-3, Q-2, R-1, S-4
(D) P-1, Q-4, R-3, S-2

**May/June 2005**

**100.** According to the guidelines for handling customer grievances related to outsourced services, what is the generally recommended time limit given to customers for forwarding their complaints?
(A) 7 days
(B) 15 days
(C) 30 days
(D) 90 days

**Oct/Nov 2024**

**101.** A large commercial bank establishes an SLA for its network operations team focusing on network functions. To manage this effectively similar to a utility, the vendor assigns a specific manager. According to the Service Level Manager (SLM) concept, how does this structure operate to benefit the bank during a network outage?
(A) The SLM manages all elements with other delivery managers, providing single-point accountability.
(B) The SLM forces the bank to contact multiple service delivery managers simultaneously.
(C) The SLM independently resets the performance measurement system without any client input.
(D) The SLM is legally shielded from reporting breaches due to internal security policies.

**May/June 2021**

**102.** A bank has outsourced its Security Operations Centre (SOC) to a third-party vendor. To maintain control and ensure regulatory compliance, what action must the bank periodically commission regarding the vendor's environment?
(A) Independent audits and expert assessments of the service provider's security environment.
(B) An internal Request for Information strictly aimed at the vendor's direct market competitors.
(C) A public disclosure of the vendor's complete structural hierarchy and internal management chain.
(D) A total reset of the established baseline performance metrics without any prior notification.

**Oct/Nov 2016**

**103.** Read the following Assertion (A) and Reason (R) and choose the correct option:
Assertion (A): During a pre-proposal conference, organization employees must not discuss the merits of a vendor's question.
Reason (R): Oral discussions surrounding a bid document bind the organization legally to modify the specifications immediately without a written addendum.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2012**

**104.** Which of the following statements about regulatory directions on the outsourcing of IT services is incorrect?
(A) The essential concept is that REs must not let outsourcing impair their capacity to meet customer responsibilities.
(B) The arrangements must remain subject to on-site and off-site monitoring by the supervising body.
(C) The RE must ensure the agreement does not obstruct effective supervision by the supervising authority.
(D) Prior authorisation from the regulator is mandatory before an RE can outsource any IT-enabled services.

**Oct/Nov 2020**

**105.** Match the named benefits of an SLA in List I with their descriptions in List II:
List I: (SLA Benefits)
P. Better communication

NODIA

productivity goals independent of the client's metrics. According to SLA management guidelines, what should the outsourcing vendor prioritize performing throughout this phase?
(A) Execute client-established workload priorities and report activities to business groups.
(B) Identify specific opportunities to improve the vendor's own internal profit margins exclusively.
(C) Pause all internal metrics reporting until the final transition-out phase formally begins.
(D) Delegate the identification of client business improvement opportunities back to the client's internal IT staff.

**Oct/Nov 2020**

**63.** Techniques for studying system performance include all of the following EXCEPT:
(A) Obfuscating workload requests
(B) Modelling
(C) Simulation
(D) Measuring real runtime system parameters

**May/June 2007**

**64.** According to regulatory guidelines, how is "outsourcing" formally defined in the context of banking?
(A) A bank's use of an internal department to perform short-term ad-hoc tasks.
(B) A bank's complete transfer of regulatory compliance to a foreign entity.
(C) A bank's use of a third party to perform activities on a continuing basis.
(D) A bank's acquisition of hardware equipment via a Request for Bid.

**Oct/Nov 2018**

**65.** What is the operational advantage for the client when the vendor's Service Level Manager (SLM) is made singularly responsible for monitoring all SLA elements and reporting on network outages?
(A) It simplifies accountability by providing the client with a single point of contact for issues.
(B) It shifts all potential financial liabilities and operational risks completely onto the client.
(C) It eliminates the need for any internal SLAs within the organization.
(D) It prevents the SLM from interacting with other service delivery managers.

**May/June 2016**

**66.** Match the banking functions in List I with their correct regulatory classification regarding outsourcing in List II:
List I: (Banking Functions)
P. KYC compliance decisions
Q. Managing investment portfolio
R. Database server maintenance
S. Application network monitoring
List II: (Classification)
1. Decision making function, cannot be outsourced.
2. Decision making function, cannot be outsourced.
3. Technology operation, can be outsourced.
4. Technology operation, can be outsourced.
(A) P-1, Q-2, R-3, S-4
(B) P-3, Q-4, R-1, S-2
(C) P-4, Q-3, R-2, S-1
(D) P-2, Q-1, R-4, S-3

**Oct/Nov 2009**

**67.** Given below are two statements regarding computing scheduling:
Statement I: In computing scheduling, goals such as maximizing throughput and minimizing latency often conflict in practice.
Statement II: A scheduler never needs to implement a compromise because user objectives universally prioritize throughput over response time.
Which of the above statement(s) is/are correct?
(A) Only Statement I
(B) Only Statement II
(C) Both Statement I and Statement II
(D) Neither Statement I nor Statement II

**May/June 2025**

**68.** Under the SMART Principle of SLA Terms, what does the "Responsible" criterion strictly dictate?
(A) Specify what resources will be consumed.
(B) Specify who will perform the action or achieve the target.
(C) Specify the legal jurisdiction of the contract.
(D) Specify the duration within which the project must conclude.

**Oct/Nov 2022**

**69.** Which of the following statistical outcomes is explicitly associated with organizations practicing the best SLA and Vendor Management?

Click Here to Buy book on Amazon

Oct/Nov 2014

**43.** Read the following Assertion (A) and Reason (R) and choose the correct option:
Assertion (A): In case of emergency changes, the change management process can be entirely bypassed to ensure immediate system recovery.
Reason (R): Emergency changes are implemented in urgency, but the entire change management process should invariably be followed post implementation of the change.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2023

**44.** Before finalizing the SLA for outsourcing a legacy application, the IT manager insists on collecting baseline performance metrics. Why is this specific activity deemed essential according to SLA best practices?
(A) It eliminates the need for any general clauses in the final contract.
(B) It legally prevents the vendor from requesting an addendum.
(C) It replaces the need to specify the Recovery Point Objective (RPO) in the agreement.
(D) It allows both parties to assess existing service levels and agree to the appropriate measures of success.

Oct/Nov 2006

**45.** Which of the following statements concerning high availability clusters and SPOFs is incorrect?
(A) A high availability cluster's effectiveness is limited by any single point of failure within its deployment.
(B) Modern servers utilize data striping across hard disks to eliminate most hardware components as a SPOF.
(C) Relying entirely on a single un-networked primary data center eliminates the risk of power outages.
(D) Real-time replication ensures that an up-to-date copy of business critical data is always available off-site.

NODIA

May/June 2010

**46.** Consider the following activities associated with the 'Commitment' phase of the SLA process:
I Assess whether an SLA is appropriate.
II Get management commitment.
III Assemble a team.
IV Create a draft SLA.
V Determine a plan to monitor the service provider.
Which combination of statements is correct?
(A) (I), (II), and (III)
(B) (II), (IV), and (V)
(C) (I), (III), and (IV)
(D) (I), (II), (IV), and (V)

Oct/Nov 2021

**47.** Even when configured with multi-pathing and shared storage (SANs), what physical element still represents a single point of failure (SPOF) that requires off-site replication to resolve?
(A) The network switch
(B) The physical data center where it is located
(C) The underlying CPU
(D) The server's error correcting memory

May/June 2015

**48.** A bank is implementing the Management phase of its newly established SLA. The IT team realizes there are many unknown variables regarding the existing data collection mechanisms for the defined KPIs. What is the recommended best approach for the team to initiate the Performance Measurement System?
(A) Immediately purchase and install a fully automated commercial tool.
(B) Start possibly with a manual data collection system and automate later after gaining experience.
(C) Suspend the SLA management phase until all variables are perfectly known.
(D) Bypass the KPI definitions and rely strictly on periodic subjective reviews.

Oct/Nov 2025

**49.** An IT vendor applies a scheduled database patch over the weekend. Unexpectedly, the patch fails and disrupts the entire production environment. To comply with sound change management processes outlined in the SLA, what should the vendor immediately execute?
(A) The clearly defined roll-back methodology to restore the environment.

their data loss, theft rates, and audit deficiencies compare to industry norms?
(A) They are equivalent to industry norms.
(B) They are half the industry norms.
(C) They are 78 percent higher than industry norm.
(D) They are twice as high as industry norms.

**May/June 2024**

**78.** The data center manager configures an alert to trigger if the CPU utilization of the Core Banking server exceeds 95% for a continuous period of 15 minutes. What type of alert configuration does this specific scenario represent?
(A) Deviation from baseline performance
(B) Predictive heuristic alert
(C) Dynamic behavioral alert
(D) Static threshold alert

**Oct/Nov 2008**

**79.** Consider the following activities to be performed by an outsourcing vendor throughout the engagement phase:
I Execute workload priorities established by the client.
II Identify opportunities to improve the client's business.
III Collect and report service level metrics.
IV Set additional productivity goals based on metrics reporting.
V Report completed and planned activities to user groups.
Which combination of statements is correct?
(A) (I), (III), and (IV), and (V)
(B) (II), (III), and (IV), and (V)
(C) (I), (II), (III), and (IV)
(D) (I), (II), (III), and (IV), and (V)

**May/June 2006**

**80.** Match the SMART Principles of SLA Terms in List I with their directives in List II:
List I: (SMART Principles)
P. Specific
Q. Measurable
R. Achievable
S. Time-related
List II: (Directives)
1. Quantify or at least suggest an indicator of progress.
2. Target a specific area for improvement.
3. Specify when the result(s) can be achieved.
4. State what results can realistically be achieved given available resources.
(A) P-2, Q-1, R-4, S-3
(B) P-1, Q-2, R-3, S-4
(C) P-4, Q-3, R-2, S-1
(D) P-2, Q-4, R-1, S-3

**Oct/Nov 2015**

**81.** According to regulatory guidelines on IT Services Outsourcing, the Board and senior management are ultimately responsible for all of the following EXCEPT:
(A) Outsourced operations.
(B) Managing risks inherent in outsourcing relationships.
(C) Directly executing the daily technical workload schedules of the vendor.
(D) Accountability for all outsourcing decisions.

**May/June 2013**

**82.** Which of the following pairs correctly matches a step in the fundamental performance monitoring strategy with its description?
(A) Baseline — Determining what constitutes "normal" performance.
(B) Collect — Establishing a baseline for unstructured data.
(C) Alert — Generating canned reports to respond to business conditions.
(D) Report — Employing static thresholds.

**Oct/Nov 2023**

**83.** Consider the following critical network areas covered by a standard SLA for a network operations team:
I Security and Finance.
II Capacity plans.
III Availability and continuity plans.
Which combination of statements is correct?
(A) (I) and (II) only
(B) (II) and (III) only
(C) (I) and (III) only
(D) (I), (II), and (III)

**May/June 2017**

**84.** Alpha Bank's board is reviewing a report from a peer group of firms categorized under the "Worst SLA and Vendor Management." If Alpha Bank falls into this category, what multiplier of business downtime compared to the industry norm is the firm statistically likely experiencing?
(A) 5 times more
(B) 13 times more

NODIA

(A) Profits that are six per cent more than industry norm.
(B) Annual revenue that is nine per cent lower than industry norm.
(C) Data loss and theft rates that are 92 per cent higher than industry norm.
(D) Business disruptions that are 63 per cent lower than industry norm.

**May/June 2018**

**70.** In the "Analyse, share and act" step of performance monitoring, proactive analysis includes all of the following actions EXCEPT:
(A) Detecting and avoiding performance events before they impact end users.
(B) Ignoring deviation from baseline alerts if they do not cause immediate downtime.
(C) Fine-tuning the infrastructure to make the most of current resources.
(D) Making more informed decisions about the impact the infrastructure has on business.

**Oct/Nov 2013**

**71.** A bank decide to outsource its core technology operations. The risk committee debates whether this non-financial process requires rigorous oversight. According to regulatory definitions, how should this specific function be classified?
(A) Material, as its disruption impacts business operations, reputation, and overall stability.
(B) A non-material technology process as it does not involve any direct financial transactions.
(C) Exempt, because technology operations fall under standard Service Level Agreement general clauses.
(D) Internal, because the transaction data originates from within the bank's own systems.

**May/June 2020**

**72.** Which of the following tools is most appropriate for analyzing network performance?
(A) PowerEdge Servers for System Performance Analysis
(B) Open NMS
(C) SolarWinds Server & Application Monitor
(D) CollectD

**Oct/Nov 2019**

**73.** Once an outsourcing project has started, what is the primary purpose of the recommended quarterly staff-planning meetings between the client and vendor?
(A) To issue new Requests for Proposals for external auditors and consultants.
(B) To finalize the initial draft of the Service Level Agreement for the parties.
(C) To legally terminate the contractual relationship transition-out phase early.
(D) To review engagement status and determine proper staffing levels and mix for subsequent quarters.

**May/June 2009**

**74.** Given below are two statements regarding SLA Implementation:
Statement I: The vendor is responsible for recommending tools and methods of automating data capture and reporting to enable an ongoing process.
Statement II: A "score card" reporting format is discouraged during the implementation phase to prevent vendor penalization.
Which of the above statement(s) is/are correct?
(A) Only Statement I
(B) Only Statement II
(C) Both Statement I and Statement II
(D) Neither Statement I nor Statement II

**Oct/Nov 2007**

**75.** Which of the following functions is incorrectly paired with its outsourcing permissibility under banking guidelines?
(A) Internal Audit — Cannot be outsourced
(B) Compliance function — Cannot be outsourced
(C) Loans sanctioning — Cannot be outsourced
(D) IT Help Desk operations — Cannot be outsourced

**May/June 2011**

**76.** Which of the following accurately describes the primary division of performance monitoring tools?
(A) Predictive and Reactive tools.
(B) Real time and Log-based tools.
(C) Analytical and Syntactical tools.
(D) Structured and Unstructured tools.

**Oct/Nov 2010**

**77.** In firms experiencing the outcomes of the "Worst SLA and Vendor Management," how do

Downloaded from www.pdf.tube

I It is the heart of the RFP.
II It is clear, complete, and logical.
III It describes the details of performance.
IV It acts as the yardstick against which vendor's performance is measured.
V It deliberately obfuscates requirements to test vendor intelligence.
Which combination of statements is correct?
(A) (I), (II), (III), and (IV)
(B) (II), (III), (IV), and (V)
(C) (I), (III), (IV), and (V)
(D) (I), (II), (IV), and (V)

**Oct/Nov 2011**

**93.** What is a specific requirement for contracting between a bank and a service provider as outlined by regulatory guidelines?
(A) Contracts must be kept strictly verbal to ensure operational flexibility.
(B) Contracts must automatically renew without periodic risk evaluation.
(C) Terms and conditions should be vetted by the bank's legal counsel on their legal effect and enforceability.
(D) Service level indicators must be excluded from the written agreement.

**May/June 2022**

**94.** A bank's project coordinator notices that a vendor is consistently delivering poor performance in maintaining the branch network. To effectively rectify this under the standard default clause, what is the most critical action the coordinator must ensure is maintained?
(A) Immediate public disclosure of the vendor's metrics.
(B) Bypassing the Purchasing Office to negotiate a new SLA.
(C) Keeping good documentation to prove the contractor is clearly at fault.
(D) Reducing the RPO to compensate for the downtime.

**Oct/Nov 2017**

**95.** A Regional Rural Bank enters into a massive IT outsourcing agreement. The vendor insists on a clause that heavily restricts the bank's access to its own core transaction logs, effectively preventing the bank from promptly responding to customer disputes. According to standard regulatory directions, why is this clause problematic?
(A) Because it reduces the SLA monitoring timeline to under 30 days.
(B) Agreements must not impair the RE's customer responsibilities or obstruct effective supervision.
(C) Because internal audits must be performed by the vendor under the new guidelines.
(D) Because the vendor must guarantee zero RPO without requiring transaction logs.

**May/June 2014**

**96.** When gauging service effectiveness, various tools are used to monitor the vendor. The metrics evaluated typically include all of the following EXCEPT:
(A) Minimum Recovery Time Objective (RTO)
(B) The precise vendor employee salary structure
(C) Recovery Point Objective (RPO)
(D) CPU utilization limits during user access time

**Oct/Nov 2005**

**97.** When should the risk evaluation of an outsourcing arrangement ideally be performed according to regulatory guidelines?
(A) Only after a massive service disruption occurs.
(B) Concurrently with the final transition-out phase.
(C) Exclusively during the internal SLA preparation phase.
(D) Prior to entering into an outsourcing agreement and reviewed periodically.

**May/June 2019**

**98.** Which statement explicitly defines the precise utility of an RFI?
(A) Used when an organization is unsure of its requirements or available market solutions.
(B) The final legally binding contract used for specific service purchase orders.
(C) The definitive standard default clause for dealing with poor vendor performance.
(D) The primary performance matrix used during the transition-out project phase.

**Oct/Nov 2012**

**99.** Match the post-proposal activities in List I with their responsible entities or actions in List II:
List I: (Post-Proposal Activities)
P. Determines proposals are complete

NODIA

goals.
4. Provides information about the contract period, validity, and termination.

(A) P-3, Q-4, R-1, S-2
(B) P-4, Q-2, R-3, S-1
(C) P-1, Q-3, R-2, S-4
(D) P-2, Q-1, R-4, S-3

**May/June 2019**

**56.** Which of the following statements regarding assembling a team for establishing an SLA is incorrect?

(A) Establishing an SLA is a process that can be carried out casually or as an afterthought once the contract begins.
(B) It requires dedicated staff to lead the effort of establishing the SLA.
(C) The team should ideally comprise an SLA Manager, Service representative(s), and a Finance representative.
(D) If applicable, other experts of relevant subject matters and a legal adviser should be included.

**Oct/Nov 2012**

**57.** Consider the following elements used to remove Single Points of Failure (SPOFs):

I Off-site replication of critical data.
II Cross-site clustering.
III Network redundancy between sites.
IV Elimination of all redundant switches to streamline traffic.

Which combination of statements is correct to achieve the highest level of availability?

(A) (I), (II), and (IV)
(B) (I), (II), and (III)
(C) (II), (III), and (IV)
(D) (I), (III), and (IV)

**May/June 2005**

**58.** Arrange the detailed sub-steps of the SLA Preparation phase in their correct chronological order:

1. Gather customer feedback
2. Assess current services
3. Determine a plan for monitoring the service provision
4. Define requirements and expectations
5. Determine working configuration and environment

(A) 2, 4, 5, 1, 3
(B) 4, 2, 1, 5, 3
(C) 2, 5, 4, 3, 1
(D) 5, 4, 2, 1, 3

**Oct/Nov 2024**

**59.** Consider the following practices regarding sound Change Management processes:

I Following a documented risk-based strategy for inventorying IT components.
II Putting in place systems to identify, track, and monitor the status of patches.
III Having a clearly defined roll-back methodology.
IV Identifying the root cause of any incident to plug vulnerabilities.
V Applying patches exclusively to end-user devices while ignoring middleware.

Which combination of statements is correct?

(A) (I), (II), III), and (IV)
(B) (II), (III), (IV), and (V)
(C) (I), (III), (IV), and (V)
(D) (I), (II), (IV), and (V)

**May/June 2021**

**60.** The structure of an SLA can broadly be divided into three main groups. Which of the following is NOT one of these main groups?

(A) General Clauses
(B) Transition-Out Workloads
(C) Services and Service Levels
(D) Management Elements

**Oct/Nov 2016**

**61.** Read the following Assertion (A) and Reason (R) and choose the correct option:

Assertion (A): It is impossible to establish baselines for unstructured data, such as system logs, within a performance monitoring platform.
Reason (R): Performance monitoring platforms require structured relational data metrics at a required granularity to function automatically.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2012**

**62.** During the operations phase of a data center management contract, the vendor sets internal

Click Here to Buy book on Amazon

Q. Guards against expectation creep
R. Mutually agreed standard
S. A process for gauging service effectiveness

List II: (Descriptions)

1. Defines standards against which the service may be measured and evaluated.
2. Identifies customer expectations, defines boundaries, and clarifies responsibilities to minimize conflicts.
3. Facilitates identification and discussion of expectations to identify achievable service levels.
4. Facilitates two-way dialogue that continues throughout the life of the arrangement.

(A) P-4, Q-3, R-2, S-1
(B) P-1, Q-2, R-3, S-4
(C) P-3, Q-4, R-1, S-2
(D) P-2, Q-1, R-4, S-3

**May/June 2007**

**106.** Given below are two statements regarding Service Provider Selection:

Statement I: Appropriate due diligence should be performed to assess the capability of the technology service provider to comply with obligations.

Statement II: Due diligence should solely involve the evaluation of the provider's financial factors, ignoring reputational and operational factors.

Which of the above statement(s) is/are correct?

(A) Only Statement I
(B) Only Statement II
(C) Both Statement I and Statement II
(D) Neither Statement I nor Statement II

**Oct/Nov 2018**

**107.** Which of the following is accurately stated regarding the definition and usage of a Request for Bid (RFB)?

(A) Used when an organization has precise requirements and knows exactly what is needed.
(B) Used when the organization does not know what is available in the marketplace.
(C) Used exclusively for internal departmental performance monitoring and reporting.
(D) A hybrid document for complex projects with potential for multiple solutions.

**May/June 2016**

**108.** When conducting due diligence on an intra-group service provider, what specific confirmation is required regarding regulatory oversight?

(A) Confirmation on the right of access to be provided to the regulator to retain effective supervision over the institution.
(B) Confirmation that the internal SLA replaces all regulatory guidelines.
(C) Confirmation that local regulatory standards do not apply to intra-group transactions.
(D) Confirmation that business continuity management is handled exclusively by the parent entity abroad.

NODIA

**Oct/Nov 2009**

**109.** Which statement regarding the pre-proposal conference is incorrect?

(A) While a pre-proposal conference is not always required, it is highly recommended.
(B) Vendors may be required to attend so that all receive the same information.
(C) A representative from the Purchasing Office typically leads the conference.
(D) If a site visit is needed, it is normally conducted prior to the issuance of the RFP document.

**May/June 2025**

**110.** By outsourcing operations and support functions to a third party, bank management fundamentally aims to achieve which of the following strategic shifts?

(A) Transferring all operational risks completely outside the organization's legal boundary.
(B) Eliminating the need to adhere to the SMART principles in future performance reviews.
(C) Gaining time for management to focus on key functions like decision making and planning.
(D) Automatically bypassing the requirement for internal Service Level Agreements.

**Oct/Nov 2022**

**111.** Read the following Assertion (A) and Reason (R) and choose the correct option:

Assertion (A): Who takes responsibility for the steps in the detailed SLA process flow depends strictly on whether the SLA is being prepared as a bilateral or trilateral agreement.

Reason (R): A trilateral agreement incorporates an additional entity, such as a regulator, into the allocation of responsibilities across the phases

timely and efficient manner.

(C) The SLA metrics must remain permanently static and unaltered regardless of dynamic business requirement changes.

(D) If service levels are consistently unmet, the reason should be established and action taken to remedy the situation.

**May/June 2013**

**124.** Using software tools to automate the SLA measuring process achieves several benefits. These benefits include all of the following EXCEPT:

(A) Eliminating the need for any regular and scheduled communication

(B) Saving time

(C) Reducing the chance of errors

(D) Reducing conflict between parties

**Oct/Nov 2023**

**125.** Regarding the regulatory directions on IT Outsourcing, which of the following statements is incorrect?

(A) The directions seek comments from Regulated Entities (REs).

(B) REs wishing to outsource IT services must seek explicit prior authorisation from the regulator for every contract.

(C) REs must ensure that outsourcing agreements do not impair their capacity to meet customer responsibilities.

(D) Outsourcing arrangements must be subject to on-site/off-site monitoring, inspection, and examination by the supervising body.



Downloaded from www.pdf.tube

providers.

May/June 2011

**118.** Consider the following requirements for banks in managing customer grievances arising from outsourced services:

I A time limit of 30 days is given to customers to forward complaints.
II The grievance redressal procedure of the bank is clearly established.
III The time frame fixed for responding to complaints is defined.
IV The procedure and time frames are placed on the bank's website.
V Customers are legally prevented from contacting the regulatory authority directly.

Which combination of statements is correct?
(A) (I), (II), (III), and (IV)
(B) (II), (III), (IV), and (V)
(C) (I), (III), (IV), and (V)
(D) (I), (II), (IV), and (V)

Oct/Nov 2010

**119.** Read the following Assertion (A) and Reason (R) and choose the correct option:
Assertion (A): The recommendation for award must address how each vendor has met or failed to meet the evaluation criteria stated in the RFP.
Reason (R): Because of the sealed competitive bid procedure, one must make objective comparative analyses of different vendor's proposals to justify the recommendation.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2024

**120.** Match the aspect of outsourcing in List I with its corresponding requirement in List II:
List I: (Outsourcing Aspects)
P. Material Outsourcing
Q. Contracting
R. Confidentiality
S. Foreign Service Providers
List II: (Requirements)
1. Must specify the minimum security baselines to be adhered to.
2. Should be carefully defined in written agreements and vetted by legal counsel.
3. Must not obstruct the ability of the regulatory authorities to perform audits based on books.
4. Refers to non-financial processes like technology operations whose disruption impacts stability.

(A) P-4, Q-2, R-1, S-3
(B) P-2, Q-4, R-3, S-1
(C) P-1, Q-3, R-2, S-4
(D) P-3, Q-1, R-4, S-2

NODIA

Oct/Nov 2008

**121.** A bank's critical database server experiences a primary motherboard failure. Instantly, the redundant element in the cluster takes over seamlessly, and users are completely unaware that a disruption even occurred. What specific capability of the facility's architecture has successfully functioned in this scenario?
(A) Network operations scheduling
(B) Change management roll-back
(C) Manual Performance Measurement tracking
(D) Fault-tolerant technology and System Resiliency

May/June 2006

**122.** Which statement regarding emergency changes in the IT environment is incorrect?
(A) A scheduled change cannot happen without undergoing the change management process.
(B) Emergency changes are implemented in urgency.
(C) The change management process should invariably be followed post implementation of the emergency change.
(D) The entire change management process can be safely ignored entirely for emergency changes even after implementation.

Oct/Nov 2015

**123.** In the final step of the Management Phase (Review SLA), which of the following actions is considered incorrect based on SLA best practices?
(A) Conducting periodic reviews of the SLA is necessary.
(B) The SLA should reflect changes in technology and customer requirements in a

the change management process cannot be entirely bypassed. Instead, the full process must invariably be followed after the change has been implemented. This ensures that the modification is properly documented, reviewed, and integrated into the system baseline, preventing future vulnerabilities and maintaining the integrity of the technical environment.

**44.** (D) It allows both parties to assess existing service levels and agree to the appropriate measures of success.
Collecting baseline performance metrics is a fundamental best practice before finalizing an SLA for outsourcing. These metrics allow both the client and the vendor to understand the existing service levels accurately. By establishing this starting point, both parties can agree on appropriate measures of success and set realistic performance targets, ensuring that future evaluations are fair and data-driven.

**45.** (C) Relying entirely on a single un-networked primary data center eliminates the risk of power outages.
High availability clusters aim to eliminate Single Points of Failure, but their effectiveness depends on the overall deployment. While modern disks use striping and real-time replication protects data off-site, relying on a single un-networked primary data center does not eliminate risk. In fact, a single site represents a major SPOF, as environmental issues like power outages could take down the entire infrastructure.

**46.** (A) (I), (II), and (III)
The Commitment phase is the initial stage of the SLA process where the foundation is laid. Key activities include assessing whether an SLA is the appropriate solution for the problem and gaining necessary management commitment. Additionally, assembling a dedicated team with relevant expertise is essential. Drafting the SLA and planning for monitoring occur in later phases like negotiation and preparation.

**47.** (B) The physical data center where it is located
Even with advanced technologies like SANs and multi-pathing, the physical data center remains a Single Point of Failure. Disasters such as fires, floods, or long-term power outages can disable the entire site regardless of internal redundancies. To resolve this, organizations must implement off-site replication and cross-site clustering, ensuring that business-critical data and applications remain available from an alternative location.

**48.** (B) Start possibly with a manual data collection system and automate later after gaining experience.
When initiating a Performance Measurement System for a new SLA, it is often best to start with a manual data collection process. This allows the team to understand the variables and refine the metrics based on experience. Once the system is stable and the requirements are clear, the organization can transition to an automated tool to save time and reduce errors.

**49.** (A) The clearly defined roll-back methodology to restore the environment.
Sound change management requires that every update has a predefined roll-back methodology. If a scheduled database patch fails and disrupts the production environment, the vendor must immediately execute this plan to restore the system to its previous stable state. This proactive approach minimizes downtime and ensures that the service provider can recover from unexpected technical issues during maintenance activities.

**50.** (C) Rewards and Remedies — General Clauses
An SLA is structured into logical groups like General Clauses, Management Elements, and Services and Service Levels. While Scope and Conventions fall under General Clauses, and Escalation Procedures are Management Elements, Rewards and Remedies are specifically part of the Services and Service Levels group. Misplacing these elements can lead to confusion regarding how performance incentives are governed within the contract.

**51.** (D) P-3, Q-4, R-2, S-1
In computing scheduling, different goals define performance. Throughput measures the total work completed per time unit, while fairness ensures equal CPU time based on priority. Latency is the time from work becoming enabled until it begins execution. Response time is the total duration between the work becoming enabled and its completion. These goals often conflict, requiring schedulers to implement compromises.

Click Here to Buy book on Amazon

# ANSWERS

1. (B) Only Statement II
A formal Request for Proposal is not required for single-source purchases that are already justified through specific procurement rules. However, an organization must issue an RFP when the required products or services exceed a specific bid limit. This occurs primarily when detailed specifications cannot completely describe the requirements due to the complexity of the intended project.

2. (A) P-2, Q-1, R-3, S-4
In a Core Banking System environment, various domains have distinct scopes. The Security Operations Centre focuses on maintaining infrastructure safety, while the Data Ware House manages historical data storage. Call Centre operations handle customer service through the Help Desk. Hardware at branches like printers and scanners falls under the peripheral domain to ensure smooth daily transactions.

3. (C) Request for Proposal
Organizations utilize a Request for Proposal as a hybrid document when they possess a general idea of requirements but lack precise specifications. It is ideal for large, complex projects where multiple solutions might exist. This tool allows vendors to propose innovative methodologies, helping the organization evaluate different approaches before finalizing a contract for the intended services.

4. (B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
Service Level Agreements enable vendors to deliver measurable results by applying orderly setup approaches. Simultaneously, these agreements provide essential methodologies for performing root cause analysis of problems. While both statements are factual regarding the benefits of outsourcing management, the provision of analysis methodologies is a separate technical advantage rather than the direct reason why results become enforceable.

5. (B) Source code of the existing legacy applications
A standard Request for Proposal document includes essential sections like task descriptions, contractor personnel requirements, and organization responsibilities. Providing the source code of existing legacy applications is not typical because this information is sensitive and usually proprietary. Organizations share such deep technical details only after selecting a vendor and signing necessary non-disclosure agreements during the implementation phase.

6. (B) Zero and near-zero
In a critical Core Banking System environment, data integrity is paramount for maintaining financial records. The Recovery Point Objective defines the maximum tolerable data loss during a disaster. For banking operations, this value should be zero or near-zero to ensure that no transactions are lost, maintaining trust and regulatory compliance while protecting the bank's overall reputation.

7. (B) Request for Information
The Request for Information is a solicitation document utilized during the early stages of procurement. It is particularly helpful when an organization lacks a clear understanding of its specific needs or is unaware of available market solutions. This process gathers information from potential vendors to help define requirements and determine if further formal bidding is necessary.

8. (B) To facilitate a comparative analysis of costs by ensuring all vendors respond to the same deliverables.
Explicitly defining deliverables within the cost proposal format of an RFP is essential for financial transparency. This structure ensures that every participating vendor responds to the exact same set of requirements. Consequently, the purchasing office can perform a fair and accurate comparative analysis of costs, ensuring that the final selection is based on standardized pricing metrics.

Downloaded from www.pdf.tube

**26.** (B) Setup, Contract, Operations, Transition-out
The life cycle of a contractual relationship follows a specific chronological sequence to ensure success. It begins with the Setup phase, followed by the formalization of the Contract. Once the agreement is signed, the relationship enters the Operations phase, where services are delivered. Finally, the Transition-out phase occurs when the contract ends or is moved to a different service provider.

**27.** (A) Expectation creep
Expectation creep occurs when one party's assumptions about the other's performance gradually become higher than what is considered reasonable or contractually agreed upon. This phenomenon can lead to significant conflict and dissatisfaction in an outsourcing relationship. A well-defined Service Level Agreement guards against this risk by explicitly outlining the boundaries of service and the specific responsibilities of each party.

**28.** (A) The Statement of Work
Within the RFP process, the Statement of Work serves as the foundational yardstick against which the vendor's actual performance is measured. It provides a clear, complete, and logical description of the tasks and performance details required. By outlining these specifics, the Statement of Work ensures that both the organization and the contractor have a shared understanding of successful delivery.

**29.** (C) Agreement between bodies within the same organization - Internal SLA
Service Level Agreements are categorized based on the relationship between the parties involved. An internal SLA exists when the agreement is between different departments or bodies within the same organization. In contrast, an external SLA is a legally binding contract between two separate organizations. Recognizing this distinction is crucial for determining the level of legal rigor and the types of remedies applicable.

**30.** (D) Proposals received after the last date of submission are marked with the time and date received and included in the bid process.
Proposal evaluation follows strict rules to ensure fairness and transparency. While proposal openings are public and vendors must be responsive to prerequisites, late submissions are treated differently. Proposals received after the designated deadline are marked with the time and date of receipt but are not included in the bid process. Adhering to these deadlines is essential for maintaining a competitive environment.

NODIA

**31.** (C) Step 3.2 Finalize SLA
Finalizing the SLA is the critical step in the negotiation phase where a formal agreement is reached. During this stage, key members from both the client and the vendor parties review the document thoroughly. They offer suggestions for improvement and reach a consensus on the final terms, ensuring that the agreement is mutually acceptable and ready for official implementation and monitoring.

**32.** (B) Ensuring application changes are managed using configuration management processes and a baseline.
A sound Change Management process ensures that application updates do not disrupt services. This involves managing changes using configuration management processes and maintaining a baseline. Additionally, having a documented risk-based strategy and a roll-back methodology is essential. These practices help identify potential issues early and provide a way to restore the system if an update fails during implementation.

**33.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Implementing Service Level Agreements should begin in selected areas where they are most needed. This phased approach is wise because if an SLA is incorrectly designed or applied to the wrong problem, it can waste resources and damage relationships. By starting small, organizations can refine their methodology and ensure that the SLA effectively solves service issues before a wider rollout.

**34.** (D) Because in some cases, the cost to correct a SPOF is costlier than the benefits of the workloads at risk.
Data center architects must balance system availability with financial constraints. In some instances, they may consciously choose not to correct an identified Single Point of Failure. This

the current arrangement while seeking improvements through regular communication.

**18.** (A) Develop and publish a Request for Proposal to evaluate multiple potential solutions.
For an upgrade as complex as a Core Banking System, a Request for Proposal is the most effective procurement methodology. Since the management expects customized solutions that vary in approach, the RFP allows vendors to propose unique methodologies. This process enables the bank to evaluate various potential solutions based on both technical merit and cost-effectiveness before making a final decision.

**19.** (D) To establish and manage expectations of customers, reducing confusion while defining acceptable service.
The primary objective of implementing a Service Level Agreement in outsourcing is to establish and manage customer expectations. By defining acceptable service levels and clarifying responsibilities, the SLA reduces confusion and potential conflicts between the parties. This document acts as a communication tool that ensures both the client and the vendor have a shared understanding of performance standards.

**20.** (D) (I), (II), and (III)
Before awarding a contract, an organization must ensure the vendor meets several prerequisites. The vendor must demonstrate business integrity and possess the necessary financial and organizational capacities to perform the work in good faith. Additionally, the submitted proposal must be responsive, meaning it conforms in all material respects to the requirements and specifications outlined in the original RFP.

**21.** (C) 70%
To ensure optimum response times for users, Service Level Agreements often stipulate specific utilization thresholds for system resources. A common industry standard is to keep CPU or memory usage at or below seventy per cent during peak access times. This buffer prevents system degradation and ensures that the infrastructure can handle sudden spikes in workload without affecting the user experience.

**22.** (B) The information received from an RFI may assist in determining whether a formal request for bid or proposal is necessary.
Different solicitation documents serve unique purposes in the purchasing process. A Request for Bid is used for precise requirements, while a Request for Proposal suits complex projects with varied solutions. Importantly, the information gathered through a Request for Information helps an organization decide whether it needs to proceed with a formal bid process or a proposal request later.

**23.** (D) To ensure all vendors receive the same information and receive constructive feedback about the RFP.
Conducting a pre-proposal conference during the RFP process ensures that all potential vendors have a consistent understanding of the requirements. This meeting provides a platform for vendors to receive the same information and offer constructive feedback. By addressing questions collectively, the organization ensures a level playing field and improves the quality of the proposals it ultimately receives from participants.

**24.** (C) (I), (II), and (IV)
Internal Service Level Agreements aim to improve organizational efficiency by boosting productivity and increasing employee morale. These agreements also assist in the development of clearer business processes between different departments. Unlike external contracts, they are not designed to facilitate legal action within the organization, but rather to foster better communication and manage expectations among various internal service providers.

**25.** (B) Only where effective competition is not available and if mentioned in the RFP document.
Negotiation after the receipt of proposals is generally restricted to maintain the integrity of the competitive bidding process. It is normally permitted only when effective competition is not available and if the possibility of negotiation was explicitly mentioned in the original RFP document. This ensures that any adjustments to terms or pricing occur within a transparent and pre-defined framework.

Click Here to Buy book on Amazon

of commitment, preparation, negotiation, and management.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2018**

**112.** Regarding Confidentiality and Security in outsourcing arrangements, what proactive measure must banks take?

(A) Allow the service provider to dictate the security baselines entirely.
(B) Define and specify minimum security baselines for service providers to protect data.
(C) Transfer legal accountability of data loss entirely to the regulatory authorities.
(D) Discontinue the use of encryption to speed up transaction throughput.

**Oct/Nov 2013**

**113.** Read the following Assertion (A) and Reason (R) and choose the correct option:

Assertion (A): Regulated Entities (REs) wishing to outsource IT and IT-enabled services do not always need to seek prior authorisation from the regulator for every contract.

Reason (R): Regulatory bodies have completely deregulated IT outsourcing, removing the requirement for any on-site/off-site monitoring, inspection, and examination by the supervising body.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2020**

**114.** The basic objectives of an internal SLA include all of the following EXCEPT:

(A) Assisting in the development of business processes.
(B) Establishing a legally binding contract that allows one department to sue another.
(C) Managing expectations and fostering good relations between departments.
(D) Boosting productivity and increasing employee morale.

**Oct/Nov 2019**

**115.** A banking institution urgently requires proprietary security software that is exclusively developed, patented, and sold by a single technology vendor globally. The purchasing department is instructed to procure this software immediately. According to standard competitive bid processes, what is the required protocol regarding the RFP?

(A) A formal RFP must be floated to multiple shell companies to simulate competition.
(B) An RFB must be used instead of an RFP.
(C) The purchase must be delayed until a competitor develops a similar software to allow for an RFP.
(D) A formal RFP is not required for justified single-source purchases.

**May/June 2009**

**116.** Consider the following characteristics of an outsourced activity used to establish management and control structures:

I Nature
II Scope
III Complexity
IV Inherent risk

Which combination of characteristics is correct?

(A) (I), (II), and (III)
(B) (II), (III), and (IV)
(C) (I), (III), and (IV)
(D) (I), (II), (III), and (IV)

NODIA

**Oct/Nov 2007**

**117.** Which statement regarding the renegotiation of internal SLAs is incorrect?

(A) An internal SLA may be less rigorous than an external SLA.
(B) The process for developing an external SLA provides a bargaining table, whereas internal renegotiating is not usually an option.
(C) Internal customers typically face the same pressures and budget constraints.
(D) An internal service provider can readily apply the exact same types of financial remedies and incentives as external

decision occurs when the cost of the corrective hardware or technology outweighs the potential benefits or the value of the specific workloads at risk. Efficiency requires prioritizing investments where they provide the most value.

**35.** (A) (I), (II), and (III)
During a phased application portfolio assessment, IT staff perform several key activities to prepare for outsourcing. These include identifying potential issues and conducting interviews with relevant IT resources to understand current operations. They also identify which applications are suitable for outsourcing. Bypassing baseline reporting is not recommended, as it is essential for measuring future success against current performance levels.

**36.** (D) (I), (II), and (III)
In data center management, a workload refers to an integrated stack of technical components required to run a specific business service. This stack typically includes the application and middleware, the underlying database, and the operating system. All these elements must function together seamlessly to deliver the intended results, making their collective management essential for maintaining high service availability and performance.

**37.** (A) Liquidation
The standard Service Level Agreement process follows a sequence of logical phases to ensure effectiveness. These include the Commitment phase for gaining management support, the Preparation phase for defining requirements, and the Management phase for monitoring performance. Liquidation is not a recognized phase of the SLA process, as the goal is ongoing service improvement rather than the termination of assets.

**38.** (A) (I) and (II) only
The Conventions section within the general clauses of an SLA provides essential definitions for the entire document. It details the specific definitions of time and identifies the meaning of key words and dates used throughout the agreement. While rewards and financial remedies are important parts of an SLA, they are typically found in separate sections focused on performance and compliance.

**39.** (D) A facility architecture feature enabling uninterrupted service delivery despite component failures.
System Resiliency refers to a facility architecture feature that allows for uninterrupted service delivery even when individual components fail. This capability is achieved through redundant systems and fault-tolerant technologies that can take over workloads instantly. In a banking environment, high resiliency is critical to ensure that hardware or software issues do not lead to noticeable service disruptions for customers.

**40.** (D) (I), (II), and (III)
The Management phase of the SLA process involves continuous oversight to ensure service quality. This includes reporting attained service levels and monitoring them through regular report reviews. Additionally, parties must periodically review the SLA itself. This review ensures the agreement remains relevant by reflecting changes in technology and evolving customer requirements, thereby maintaining a high standard of service delivery.

**41.** (B) It can run in physical, virtual, or cloud computing environments.
When a workload is described as platform independent, it means the software stack can operate across various computing environments. It is not restricted to specific hardware like physical mainframes. Instead, it can run efficiently in physical, virtual, or cloud-based infrastructures. This flexibility is vital for modern data centers, allowing for easier migration and scalability as business requirements and technologies evolve.

**42.** (A) P-4, Q-3, R-1, S-2
In the SLA preparation phase, different steps serve specific goals. Assessing current services helps determine realistic levels before making commitments, while checking the configuration verifies if the environment impacts service. Gathering customer feedback provides a baseline for satisfaction, and planning for monitoring involves drafting Key Performance Indicators. These steps collectively ensure that the final agreement is grounded in operational reality.

**43.** (D) Assertion (A) is false, but Reason (R) is true.
While emergency changes require immediate implementation to restore critical systems,

Downloaded from www.pdf.tube

**9.** (A) Only Statement I
Internal Service Level Agreements are generally considered less rigorous than external ones because renegotiation is often not a feasible option for internal customers. Furthermore, internal service providers cannot easily apply the same financial penalties or remedies used with external vendors. These agreements primarily serve to manage expectations and improve communication between different departments within the same organization.

**10.** (C) It cannot be relied upon unless it is documented in a written addendum to the bid document.
During a pre-proposal conference, any verbal information provided by organization representatives regarding technical requirements does not hold contractual weight. Vendors cannot legally rely on oral clarifications that materially affect the bid document. To become binding, such information must be formally documented and issued as a written addendum to the original solicitation by the purchasing office.

**11.** (D) It results in substantial financial gains for the client in the operations and exit phases.
Investing significant resources during the initial setup and contract stages of an SLA leads to long-term efficiency. While these early phases require more time and money, they prevent costly misunderstandings and service failures later on. This proactive approach ultimately results in substantial financial gains for the client during the operational and transition-out phases of the vendor relationship.

**12.** (C) Setup and Contract
Ensuring a smooth transition-out and operational phase depends heavily on the groundwork laid during the setup and contract stages. These two early phases require intense focus to define clear expectations, metrics, and legal obligations. By establishing a robust framework at the start, organizations minimize potential conflicts and ensure the outsourcing engagement meets its intended business and technical objectives.

**13.** (A) The standard default clause
When a vendor consistently fails to meet agreed-upon performance timelines, the organization uses the standard default clause to initiate corrective actions. This provision allows the project coordinator to issue a formal notice demanding a resolution plan within a specific period. Maintaining detailed documentation is vital during this process to prove the contractor's fault and justify further legal or administrative actions.

**14.** (C) Assertion (A) is true, but Reason (R) is false.
An evaluation matrix serves as a critical tool for individuals responsible for scoring vendor proposals based on pre-defined criteria. It ensures the selection process remains objective and structured. However, this matrix does not allow organizations to bypass sealed competitive bid procedures. Instead, it supports the integrity of the process by ensuring all vendors are measured against the same standards.

**15.** (D) The time taken to resume operations in case of a disaster.
In a Core Banking System environment, the Recovery Time Objective represents the duration within which business operations must be restored after a disaster occurs. It focuses on minimizing downtime to ensure service availability for customers. Unlike data loss metrics, this objective sets a clear deadline for the technical team to bring the systems back to a functional state.

**16.** (A) Request for Bid
A Request for Bid is the appropriate solicitation document when an organization has formulated precise requirements and specifications. Because the organization knows exactly what it needs, the focus shifts to finding the best price for the defined service. This document is less flexible than a proposal request and is typically used for well-defined products or standardized technical services.

**17.** (A) Terminate the contract, renegotiate terms, or continue with the existing arrangement.
When a vendor repeatedly fails to meet guaranteed service levels in an external SLA, the client has several contractual options. Depending on the agreement terms, the bank may choose to terminate the contract for default or renegotiate more realistic metrics. Alternatively, if the impact is manageable, the bank might continue

**52.** (D) SLA Catalogue and SLA Guidance Material
During the SLA Negotiation phase, using a template helps standardise the agreement. To further aid the drafting process, parties should consult the SLA Catalogue and SLA Guidance Material. These resources provide standardized service descriptions and expert advice on best practices, helping both the vendor and the client reach a clear, effective, and mutually beneficial agreement that can be tested early.

**53.** (C) The Regulator
A trilateral Service Level Agreement involves three distinct parties working together. In a banking or financial context, this typically includes the organization, the data originator, and the regulator. The inclusion of the regulator ensures that the agreement meets all necessary compliance standards and that the oversight body can effectively monitor the outsourcing arrangement according to established legal and operational guidelines.

**54.** (A) P-1, Q-4, R-2, S-3
Different architecture concepts address specific operational needs. Fault tolerance prevents catastrophic failures from logic errors, while server clustering allows duplicate applications to run if one server fails. Redundant switches provide alternative network paths to prevent disconnects. Conversely, a Single Point of Failure is a risk that can compromise entire workloads or the whole data center if it is not properly addressed.

**55.** (A) P-3, Q-4, R-1, S-2
Each component of an SLA serves a specific descriptive purpose. The Scope agrees upon the quality and quantity of services, while the Term defines the contract period and validity. Conventions detail the definitions of time and key words used in the document. Finally, the Parties to the Agreement section identifies the legal entities and persons responsible for the contractual relationship.

**56.** (A) Establishing an SLA is a process that can be carried out casually or as an afterthought once the contract begins.
Establishing a Service Level Agreement is a formal process that requires dedicated staff and careful planning. It cannot be treated casually or as an afterthought once operations have already begun. A successful team should include an SLA Manager, service and finance representatives, and legal advisers to ensure that all technical, financial, and legal aspects of the agreement are thoroughly addressed.

**57.** (B) (I), (II), and (III)
Achieving the highest level of system availability requires eliminating Single Points of Failure at multiple levels. This is done through off-site replication of critical data and implementating cross-site clustering for applications. Additionally, maintaining network redundancy between different sites ensures continuous connectivity. Removing redundant switches would actually create a new SPOF, contradicting the goal of maximizing infrastructure resilience and service uptime.

**58.** (A) 2, 4, 5, 1, 3
The SLA Preparation phase follows a logical order to ensure all requirements are met. It begins by assessing current services and defining expectations. Next, the team determines the working configuration and environment. After these technical steps, they gather customer feedback to provide a baseline for satisfaction. Finally, they determine a plan for monitoring the service provision before finalizing the agreement.

**59.** (A) (I), (II), III), and (IV)
Sound Change Management involves several critical practices to protect the IT environment. These include following a risk-based inventory strategy and tracking the status of all patches. A clearly defined roll-back methodology is essential for recovery if changes fail. Additionally, identifying the root cause of incidents helps prevent future vulnerabilities. These practices should be applied comprehensively across all systems, including middleware.

**60.** (B) Transition-Out Workloads
The structure of a standard Service Level Agreement is organized into three primary groups: General Clauses, Services and Service Levels, and Management Elements. These categories ensure that all legal, technical, and operational aspects are covered. While transition-out is a phase in the contract life cycle, it is not considered one

Click Here to Buy book on Amazon

leaving specialized technical tasks to experienced third-party service providers.

**111.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Responsibility for the steps in the detailed SLA process flow is determined by the type of agreement being prepared. In a bilateral agreement, responsibilities are shared between the organization and the vendor. However, a trilateral agreement introduces a third entity, such as a regulator. This addition changes how tasks are allocated across the Commitment, Preparation, Negotiation, and Management phases of the relationship.

**112.** (B) Define and specify minimum security baselines for service providers to protect data.
To protect sensitive data in an outsourcing arrangement, banks must take a proactive role in security. They are required to define and specify minimum security baselines that the service provider must adhere to. This ensures that all data handled by the third party is protected according to the bank's standards, rather than relying solely on the vendor's internal security policies and procedures.

**113.** (C) Assertion (A) is true, but Reason (R) is false.
Regulated entities do not need prior authorisation from the regulator for every individual IT outsourcing contract. However, it is false to say that regulatory bodies have completely deregulated this area. On the contrary, all outsourcing arrangements remain subject to strict on-site and off-site monitoring by supervising authorities to ensure that banks maintain high standards of risk management and operational resilience.

**114.** (B) Establishing a legally binding contract that allows one department to sue another.
Internal Service Level Agreements serve several operational goals, such as assisting in business process development and managing expectations between departments. They also aim to boost productivity and morale by clarifying roles. However, unlike external contracts, they are not designed to create a legally binding environment where one department can sue another. Instead, they provide a framework for internal collaboration and communication.

**115.** (D) A formal RFP is not required for justified single-source purchases.
When a bank needs a proprietary product that is only available from a single global vendor, a traditional competitive bidding process is not possible. In such cases of justified single-source purchases, a formal Request for Proposal is not required. The purchasing department can proceed directly with the procurement, provided they have properly documented the reasons why no other alternative solutions or vendors exist.

**116.** (D) (I), (II), (III), and (IV)
When establishing management and control structures for an outsourced activity, several characteristics must be considered. These include the nature and scope of the work, along with its technical complexity. Furthermore, the inherent risk associated with the activity is a critical factor. Evaluating all these characteristics ensures that the bank implements an oversight framework that is appropriate for the specific outsourcing engagement.

**117.** (D) An internal service provider can readily apply the exact same types of financial remedies and incentives as external providers.
Internal Service Level Agreements differ from external ones in several ways. They may be less rigorous, and internal customers often lack a formal bargaining table for renegotiation. Crucially, internal service providers cannot readily apply the exact same types of financial remedies and incentives that external providers do. This is because all departments usually operate within the same overall organizational budget and management structure.

NODIA

**118.** (A) (I), (II), (III), and (IV)
Banks must maintain clear customer grievance procedures for outsourced services, including a thirty-day limit for customers to file complaints. These procedures and response timeframes must be prominently displayed on the bank's website. While the bank provides its own redressal mechanism, customers are never legally prevented from contacting the regulatory authority directly if they are dissatisfied with how their complaint was handled.

see significant financial benefits. Research indicates that these firms achieve profits that are six per cent higher than the industry norm. This success stems from reduced business disruptions and more efficient service delivery, demonstrating that strong contractual oversight and performance monitoring contribute directly to an organization's overall financial health.

**70.** (B) Ignoring deviation from baseline alerts if they do not cause immediate downtime.
Proactive performance analysis involves several key actions to maintain system health. This includes detecting and avoiding performance events before they impact users and fine-tuning infrastructure for better resource utilization. However, ignoring alerts regarding deviations from the baseline is not a proactive practice. Such deviations often serve as early warning signs of potential future downtime and must be addressed promptly.

**71.** (A) Material, as its disruption impacts business operations, reputation, and overall stability.
Even though core technology operations are non-financial processes, they are classified as material outsourcing. This is because any disruption to these services can significantly impact the bank's business operations, reputation, and overall stability. Regulatory bodies require rigorous oversight for such functions to ensure that the bank remains resilient and can continue serving its customers without interruption.

**72.** (B) Open NMS
For analyzing network performance, Open NMS is one of the most appropriate and widely used tools. It is designed specifically to monitor network connectivity and performance across diverse infrastructures. While other tools like SolarWinds or CollectD might focus on servers or applications, Open NMS provides the specialized features needed to track network health and ensure high availability for interconnected systems.

**73.** (D) To review engagement status and determine proper staffing levels and mix for subsequent quarters.
Once an outsourcing project is operational, quarterly staff-planning meetings between the client and vendor are essential. The primary purpose of these meetings is to review the current engagement status and determine the appropriate staffing levels and mix for the upcoming quarters. This ensures that the vendor has the right resources in place to meet the evolving needs of the bank.

**74.** (A) Only Statement I
During SLA implementation, the vendor is responsible for recommending tools to automate data capture and reporting. This enables a consistent and ongoing monitoring process. Contrary to some assumptions, using a score card reporting format is actually encouraged. It provides a clear and structured way to visualize performance against targets, helping both parties identify areas that require improvement or corrective action.

**75.** (D) IT Help Desk operations — Cannot be outsourced
Banking guidelines specify which functions can and cannot be outsourced. Core responsibilities like internal audit, compliance functions, and loan sanctioning must remain within the bank. However, IT Help Desk operations are technical services that are perfectly suitable for outsourcing. Misclassifying the Help Desk as a non-outsourceable function ignores common industry practices for improving technical support through specialized third-party providers.

**76.** (B) Real time and Log-based tools.
Performance monitoring tools are broadly divided into two main categories: real-time tools and log-based tools. Real-time tools provide immediate visibility into current system behavior, allowing for quick responses to issues. Log-based tools analyze historical data recorded in system logs to identify trends and perform root cause analysis. Using both types ensures a comprehensive understanding of both present and past performance.

**77.** (D) They are twice as high as industry norms.
Firms that experience the worst Service Level Agreement and vendor management outcomes face severe operational risks. Statistical data shows that these organizations have data loss, theft rates, and audit deficiencies that are twice as high as industry norms. This highlights the critical importance of implementing robust

NODIA

project coordinator must prioritize thorough documentation. Clear evidence proving that the contractor is at fault for failing to meet timelines or service quality is essential. This documentation supports the issuance of formal notices and protects the bank's interests during any subsequent legal disputes or contract termination processes.

**95.** (B) Agreements must not impair the RE's customer responsibilities or obstruct effective supervision.
Clauses that restrict a bank's access to its own transaction logs are problematic because they impair the institution's ability to meet customer responsibilities. Furthermore, such restrictions can obstruct effective supervision by regulatory authorities. Agreements must ensure that the bank remains in control of its data to resolve customer disputes promptly and allow regulators to perform necessary inspections and audits without hindrance.

**96.** (B) The precise vendor employee salary structure
Monitoring a vendor's service effectiveness involves evaluating various technical and operational metrics. Key indicators include the Recovery Time Objective, the Recovery Point Objective, and CPU utilization limits during user access times. However, the precise internal salary structure of the vendor's employees is not a standard metric for gauging service performance and is generally considered outside the scope of the client's monitoring activities.

**97.** (D) Prior prior to entering into an outsourcing agreement and reviewed periodically.
According to regulatory guidelines, a bank should perform a risk evaluation of any outsourcing arrangement before entering into the agreement. This proactive assessment helps identify potential threats to business continuity or data security. Furthermore, these evaluations must be reviewed periodically throughout the life of the contract to account for changes in the operational environment, technology, or regulatory requirements.

**98.** (A) Used when an organization is unsure of its requirements or available market solutions.
A Request for Information is a valuable tool used when an organization is unsure of its specific requirements or the solutions currently available in the marketplace. It allows the purchasing office to gather broad information from various vendors without committing to a purchase. The insights gained from an RFI help the organization define its needs more clearly before moving to a formal RFP.

**99.** (A) P-2, Q-3, R-4, S-1
After proposals are received, different entities handle specific tasks. The Purchasing Office determines if proposals are complete, while department or committee members evaluate them against set criteria. The Purchasing department then agrees on the awarded firm based on these evaluations. Once the contract begins, department monitors are responsible for tracking the contractor's performance to ensure all service obligations are met.

**100.** (C) 30 days
For the effective handling of customer grievances in an outsourced banking environment, the institution must define a clear procedure. This includes setting specific time limits for when a customer should forward their complaint. The generally recommended timeframe is thirty days, ensuring that issues are addressed while the details of the transaction or service failure are still fresh and verifiable.

**101.** (A) The SLM manages all elements with other delivery managers, providing single-point accountability.
During a network outage, the Service Level Manager structure provides a major benefit by ensuring single-point accountability. The SLM manages all elements of the SLA and coordinates with other internal service delivery managers to resolve the issue. This centralized approach prevents the bank from having to interact with multiple contacts, leading to faster resolution times and clearer communication during critical disruptions.

**102.** (A) Independent audits and expert assessments of the service provider's security environment.
When a bank outsources its Security Operations Centre, it must maintain rigorous oversight to ensure regulatory compliance and data protection. This involves periodically commissioning independent audits and expert assessments of

Downloaded from www.pdf.tube

**86.** (B) VTune Performance Analyzer and Iometer
When analyzing the Input/Output performance of servers, specific specialized tools are required. VTune Performance Analyzer and Iometer are both highly effective for this purpose. Iometer is widely used to measure I/O subsystem performance under various workloads, while VTune helps identify performance bottlenecks at a deeper level. These tools provide the technical data needed to optimize data storage and retrieval processes.

**87.** (B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
Outsourcing allows bank management to focus on core functions like planning and decision-making by delegating routine operations. The benefits of this approach include operational efficiencies and faster access to modern technology. While both statements are true regarding why banks outsource, the list of general operational benefits is a separate factual point rather than the direct reason why management time specifically increases.

**88.** (C) Because metrics like voltage or temperature cause failures if they fall outside a specific range.
Effective performance monitoring requires the ability to set both upper and lower-level ranges for certain alerts. This is because some critical environmental metrics, such as voltage or temperature, can cause system failures if they either rise too high or fall too low. Monitoring a range rather than just a single threshold ensures that the infrastructure operates within safe and stable parameters.

**89.** (B) 10%
According to recent surveys, only ten per cent of total organizations have implemented the best Service Level Agreement and vendor management practices. This elite group achieves significantly higher profits and much lower business disruptions compared to their peers. This statistic suggests that there is substantial room for improvement in how most organizations handle their outsourcing contracts and performance monitoring efforts.

**90.** (D) The process must hide the reasons for unmet SLAs from the steering committee to preserve vendor relations.
A transparent reporting process is vital for successful SLA implementation. The process should identify where service levels are not being met and report these findings back to a steering committee. It is incorrect to suggest that the reasons for unmet SLAs should be hidden from the committee. Understanding the root causes of performance failures is essential for implementing effective remedies and improvements.

**91.** (B) The vendor's ability to maximize their operational profits.
When outsourcing to an international service provider, a bank must ensure that the arrangement does not hinder regulatory oversight. This includes maintaining the regulator's ability to perform audits and reconstruct activities from books and records. While the bank must facilitate timely access to documentation for supervisors, it is not responsible for ensuring the vendor's ability to maximize their internal operational profits.

NODIA

**92.** (A) (I), (II), (III), and (IV)
The Scope of Work is the heart of an RFP and must be clear, complete, and logical. It describes the precise details of performance and acts as the yardstick for measuring vendor success. Deliberately obfuscating requirements would be counterproductive, as the goal is to ensure vendors fully understand the needs so they can propose the most effective and accurate solutions.

**93.** (C) Terms and conditions should be vetted by the bank's legal counsel on their legal effect and enforceability.
Regulatory guidelines require that the terms and conditions of an outsourcing contract be thoroughly vetted by the bank's legal counsel. This review ensures that the agreement has the intended legal effect and is fully enforceable. A written contract is mandatory, and it must include specific service level indicators to provide a clear framework for monitoring the provider's performance and accountability.

**94.** (C) Keeping good documentation to prove the contractor is clearly at fault.
To effectively use the standard default clause against a poorly performing vendor, the

SLA frameworks and active vendor oversight to protect sensitive data and maintain regulatory compliance.

**78.** (D) Static threshold alert
A static threshold alert is triggered when a specific metric exceeds a pre-defined fixed value for a certain duration. In this scenario, the alert is set for CPU utilization exceeding ninety-five per cent for fifteen minutes. This type of configuration is straightforward and helps administrators identify when a system is under excessive load that could lead to performance degradation or failure.

**79.** (D) (I), (II), (III), and (IV), and (V)
Throughout an outsourcing engagement, the vendor performs several critical activities to ensure success. These include executing client-established workload priorities and identifying opportunities for business improvement. The vendor must also collect and report service level metrics while setting additional productivity goals based on those reports. Finally, reporting all planned and completed activities to user groups maintains transparency and trust.

**80.** (A) P-2, Q-1, R-4, S-3
The SMART principles provide a framework for clear SLA terms. Specific targets a particular area for improvement, while Measurable involves quantifying progress. Achievable ensures that results are realistic given the available resources. Finally, Time-related specifies the timeframe within which the results should be achieved. These principles ensure that performance expectations are well-defined and manageable for both parties involved.

**81.** (C) Directly executing the daily technical workload schedules of the vendor.
In an outsourcing relationship, the Board and senior management of a bank retain ultimate responsibility for all outsourced operations and the management of inherent risks. They are also accountable for all outsourcing decisions. However, they are not expected to directly execute the daily technical workload schedules of the vendor. That operational task remains the responsibility of the service provider's management team.

**82.** (A) Baseline — Determining what constitutes "normal" performance.
A fundamental performance monitoring strategy begins with establishing a baseline, which involves determining what constitutes normal performance for the system. This baseline acts as the standard against which future performance is measured. Other steps include collecting data, generating alerts when performance deviates from the norm, and reporting results to stakeholders. Correctly identifying normal behavior is essential for accurate anomaly detection.

**83.** (D) (I), (II), and (III)
A standard Service Level Agreement for a network operations team covers several critical areas to ensure robust infrastructure. These include security and finance considerations to protect data and manage costs. The agreement also addresses capacity plans to handle future growth, along with availability and continuity plans. These elements combined ensure that the network remains reliable and secure for all business transactions.

**84.** (C) 25 times more
Organizations categorized under the Worst SLA and Vendor Management face significant operational challenges. Statistical reports indicate that these firms experience business downtime that is twenty-five times higher than the industry norm. This massive disparity underscores how poor contractual management and a lack of effective performance monitoring can lead to catastrophic service interruptions and substantial financial losses for the institution.

**85.** (D) (I), (II), (III), and (IV)
To effectively address service level challenges, organizations leverage several management elements. This includes involving named executives and management participants to ensure leadership support. Defining measurable commitments and establishing clear escalation procedures provides a path for resolving issues. Finally, maintaining regular and scheduled communication ensures that both the client and the vendor stay aligned on performance goals and operational requirements.

Click Here to Buy book on Amazon

the service provider's security environment. These evaluations provide an objective view of the vendor's performance and help identify any vulnerabilities that could compromise the bank's infrastructure or sensitive customer information.

**103.** (C) Assertion (A) is true, but Reason (R) is false.
During a pre-proposal conference, organization employees must avoid discussing the relative merits of any vendor's question to maintain impartiality. While oral discussions occur, they do not legally bind the organization to change specifications. Only a written addendum issued by the purchasing office can modify the original bid document, ensuring that all participating vendors have access to the same formal information.

**104.** (D) Prior authorisation from the regulator is mandatory before an RE can outsource any IT-enabled services.
Regulatory guidelines on outsourcing emphasize that banks must not impair their capacity to meet customer responsibilities. While outsourcing arrangements are subject to on-site and off-site monitoring by supervising bodies, it is incorrect to state that prior authorisation is mandatory for every single IT-enabled service contract. Banks are generally expected to manage these relationships within a pre-defined framework of risk and compliance.

**105.** (A) P-4, Q-3, R-2, S-1
Different benefits of an SLA address various aspects of the vendor relationship. Better communication facilitates an ongoing two-way dialogue. Guarding against expectation creep helps identify boundaries and clarifies responsibilities. A mutually agreed standard provides the basis for measuring service, while a process for gauging effectiveness facilitates the identification and discussion of expectations to ensure that all service levels remain achievable and measurable.

**106.** (A) Only Statement I
Due diligence is a mandatory step in selecting a technology service provider. It involves assessing the provider's capability to comply with all contractual and regulatory obligations. Contrary to focusing only on financial factors, a comprehensive due diligence process must also evaluate reputational and operational factors. This holistic approach ensures the vendor is reliable and capable of delivering high-quality services over the long term.

**107.** (A) Used when an organization has precise requirements and knows exactly what is needed.
A Request for Bid is utilized when an organization knows exactly what it needs and has formulated precise requirements. This document is focused on obtaining the best price for a well-defined product or service. Unlike a Request for Proposal, it leaves little room for vendor-proposed alternative solutions, making it ideal for standard technical requirements where the specifications are clearly established and understood.

**108.** (A) Confirmation on the right of access to be provided to the regulator to retain effective supervision over the institution.
When a bank uses an intra-group service provider, especially one located in a different jurisdiction, it must ensure that regulatory oversight is not compromised. The bank must obtain confirmation that the regulator will have a right of access to the provider. This ensures that the supervising body can maintain effective oversight over the bank's operations, regardless of the provider's internal relationship.

NODIA

**109.** (D) If a site visit is needed, it is normally conducted prior to the issuance of the RFP document.
A pre-proposal conference is a recommended meeting where the purchasing office shares information with all vendors simultaneously. While highly beneficial, it is not always mandatory. If a site visit is required to help vendors understand the scope of work, it is normally conducted after the RFP document has been issued, allowing vendors to relate the physical environment to the written requirements.

**110.** (C) Gaining time for management to focus on key functions like decision making and planning.
By outsourcing routine operations and support functions, bank management aims to achieve a strategic shift in how they spend their time. The goal is to free up management resources to focus on key functions such as decision-making, planning, and business development. This allows the bank to improve its overall performance while

of the three main structural groups of the SLA document itself.

**61.** (D) Assertion (A) is false, but Reason (R) is true.
It is possible to establish baselines for unstructured data, such as system logs, within modern performance monitoring platforms. These tools are designed to ingest and analyze various data types. However, to function automatically and provide granular insights, these platforms do require structured relational data metrics. This allows them to effectively compare current performance against historical norms and trigger relevant alerts.

**62.** (A) Execute client-established workload priorities and report activities to business groups.
During the operations phase of an outsourcing contract, the vendor must align its activities with the client's business goals. This involves prioritizing workloads established by the client and reporting all activities back to user groups. The vendor should also actively identify opportunities to improve the client's business processes, ensuring that the engagement provides ongoing value beyond simple task execution.

**63.** (A) Obfuscating workload requests
Professionals use various techniques to study system performance and ensure efficiency. Common methods include modeling to predict behavior and simulation to test scenarios. Additionally, measuring real runtime system parameters provides accurate data on current performance. Obfuscating workload requests is not a recognized technique for performance analysis, as it would intentionally hide necessary data rather than clarifying system behavior.

**64.** (C) A bank's use of a third party to perform activities on a continuing basis.
Regulatory guidelines formally define outsourcing as a bank's use of a third party to perform activities on a continuing basis. These activities would normally be undertaken by the bank itself, either now or in the future. This definition emphasizes the long-term nature of the relationship and the transfer of operational responsibility for specific functions to an external service provider.

**65.** (A) It simplifies accountability by providing the client with a single point of contact for issues.
Assigning a specific Service Level Manager to be responsible for monitoring all SLA elements provides a significant operational advantage. It simplifies accountability by giving the client a single point of contact for all issues, including network outages. This structure ensures that the SLM can coordinate with other service delivery managers internally while providing clear and consistent reporting to the bank.

**66.** (A) P-1, Q-2, R-3, S-4
In banking, functions are classified based on their suitability for outsourcing. Core decision-making tasks, such as KYC compliance decisions and managing investment portfolios, cannot be outsourced because they involve institutional responsibility. In contrast, technology operations like database server maintenance and application network monitoring can be outsourced to specialized third-party vendors to improve efficiency and leverage external expertise.

**67.** (A) Only Statement I
In computing scheduling, goals like maximizing throughput and minimizing latency often conflict because improving one can negatively impact the other. For instance, increasing throughput might lead to higher latency for individual tasks. Therefore, schedulers must frequently implement compromises based on user objectives. It is incorrect to say users always prioritize throughput, as different applications have varying requirements for response time.

**68.** (B) Specify who will perform the action or achieve the target.
Under the SMART principles for defining SLA terms, the Responsible criterion is critical for accountability. It strictly dictates that the agreement must specify exactly who will perform a given action or be accountable for achieving a specific performance target. This clarity ensures that both the client and the vendor know which individuals or teams are responsible for meeting service obligations.

**69.** (A) Profits that are six per cent more than industry norm.
Organizations that practice the best Service Level Agreement and vendor management

Downloaded from www.pdf.tube

**119.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
A formal recommendation for award must detail how each vendor met or failed to meet the specified evaluation criteria. Because of the sealed competitive bid procedure, this objective comparative analysis is essential. It provides a transparent justification for the final selection, ensuring that the process remains fair and that the chosen vendor is the one best suited to meet the organization's needs.

**120.** (A) P-4, Q-2, R-1, S-3
Different aspects of outsourcing involve specific requirements. Material outsourcing refers to non-financial processes whose disruption impacts stability. Contracting involves written agreements vetted by legal counsel. Confidentiality requires specifying minimum security baselines for data protection. Finally, dealing with foreign service providers must not obstruct the ability of regulatory authorities to perform audits and inspections based on the bank's records and books.

**121.** (D) Fault-tolerant technology and System Resiliency
When a redundant element in a cluster takes over instantly after a hardware failure, it demonstrates the effectiveness of fault-tolerant technology. This capability is part of overall system resiliency, which ensures that services remain uninterrupted for users despite component failures. In a banking environment, such features are essential for maintaining high availability and preventing noticeable disruptions during critical daily financial operations.

**122.** (C) The change management process should invariably be followed post implementation of the emergency change.
While emergency changes are often implemented with great urgency to restore critical banking services, the change management process cannot be entirely bypassed. Instead, the full process must invariably be followed after the change has been implemented. This ensures that the modification is properly documented, reviewed, and integrated into the system baseline, preventing future vulnerabilities and maintaining the integrity of the technical environment.

**123.** (C) The SLA metrics must remain permanently static and unaltered regardless of dynamic business requirement changes.
In the final review stage of the management phase, it is critical to ensure the Service Level Agreement remains relevant to the current business environment. Technology and customer needs evolve over time, necessitating periodic updates to performance metrics. Suggesting that these indicators should remain permanently static is incorrect, as it prevents the agreement from addressing new challenges effectively.

**124.** (A) Eliminating the need for any regular and scheduled communication
Automating the measurement process using specialized software tools provides several benefits, including time savings and a reduction in manual calculation errors. It also provides objective data that helps minimize conflicts. However, technology cannot replace human oversight. Regular and scheduled communication between the parties remains a vital requirement for managing the overall relationship and addressing complex service issues.

**125.** (B) REs wishing to outsource IT services must seek explicit prior authorisation from the regulator for every contract.
Regulatory guidelines on IT services focus on ensuring that banks maintain control over their operations and meet customer responsibilities. These arrangements are subject to ongoing on-site and off-site monitoring by supervisors. However, the requirement is not so restrictive that every single contract needs explicit prior authorisation. Banks are instead expected to operate within the established regulatory risk-management framework.

NODIA

www.nodia.in

# CHAPTER 20

# RBI Guidelines on Cyber Security & Digital Payment Security

**Oct/Nov 2025**

**1.** Arrange the following regulatory developments and reporting deadlines in chronological order:

I Submission of gaps and viable plan by CISO to RBI

II RBI circular based on the G. Gopalakrishna Committee recommendations

III Implementation of Master Directions on Digital Payment Security Controls

IV Communication of Cyber Security Policy to the CSITE Cell

(A) (II), (I), (IV), (III)
(B) (I), (II), (III), (IV)
(C) (II), (IV), (I), (III)
(D) (IV), (II), (I), (III)

**May/June 2018**

**2.** Which government entity in India has been taking important initiatives in strengthening cyber-security by providing proactive & reactive services, threat intelligence, and assessment guidelines?

(A) IB-CART
(B) ReBIT
(C) CERT-In
(D) IDRBT

**Oct/Nov 2014**

**3.** Which IT Subsidiary has the Reserve Bank of India created specifically to cater to its IT and cyber security needs and to ensure the cyber resilience of Indian banking?

(A) Indian Banks – Center for Analysis of Risks and Threats (IB-CART)
(B) Computer Emergency Response Team - India (CERT-In)
(C) Reserve Bank Information Technology Pvt. Ltd. (ReBIT)
(D) Cyber Security and Information Technology Examination (CSITE) Cell

**May/June 2021**

**4.** What is the conceptual benefit of participating in activities like the CISOs' Forum and IB-CART?

(A) It shifts the liability of cyber incidents from individual banks to IDRBT and other central entities.
(B) It provides an avenue for banks to market their proprietary digital payment applications and services.
(C) It facilitates collective threat intelligence and the adoption of proactive cyber security measures.
(D) It replaces the need for an internal Security Operations Centre (SOC) through external collaboration.

**Oct/Nov 2009**

**5.** What is the most appropriate reason for requiring a bank's Cyber Security Policy to be separate from its broader IS Security policy?

(A) To justify the appointment of a dedicated Chief Information Security Officer (CISO) and support staff.
(B) To highlight specific cyber risks and the corresponding measures required to mitigate these threats.
(C) To comply with international standards such as PCI-DSS and ISO 27001 within the regional framework.
(D) To ensure that the traditional BCP/DR arrangements are entirely replaced by modern digital protocols.

**May/June 2016**

**6.** Consider the following statements regarding the Supervisory Reporting Framework:

I It has been decided to collect only summary level information regarding cyber-incidents to minimize administrative burden.

II The framework mandates the collection of both summary level information as well as

Click Here to Buy book on Amazon

details on information security incidents.

Which of the above statement(s) is/are correct?

(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**Oct/Nov 2023**

**7.** Which of the following best defines the primary focus of Information Security as distinguished from Cyber Security?

(A) The ability to protect or defend the use of cyberspace from cyberattacks through proactive defenses.
(B) Protecting the confidentiality, integrity, and availability of information assets.
(C) Addressing risks emanating from cyber warfare and interconnected internet of things devices.
(D) Managing negative social impacts and risks from the interaction of people on the internet.

**May/June 2011**

**8.** Consider the following statements regarding Network and Database Security:

I Connections to networks/databases allowed for a specified period of time often remain open due to oversight.
II Unauthorized access to networks and databases must be completely disallowed.
III Responsibility over networks and databases can be entirely outsourced to vendors to mitigate bank liability.

Which of the above statement(s) is/are correct?

(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) (I), (II), and (III)

**Oct/Nov 2018**

**9.** Match the items in List I with those in List II:

List I: (Cyber Threats)

P. Vishing
Q. DDoS
R. Whaling
S. Drive-by downloads

List II: (Characteristics or Methods)

1. Overwhelming a system's resources to cause denial of service
2. A form of voice-based phishing to extract confidential data
3. Unintended execution or downloading of malware from compromised websites
4. Highly targeted phishing attacks directed at senior executives

(A) P-2, Q-1, R-4, S-3
(B) P-1, Q-2, R-3, S-4
(C) P-4, Q-3, R-2, S-1
(D) P-3, Q-4, R-1, S-2

**May/June 2024**

**10.** A mid-sized commercial bank is updating its internal policies. The Chief Information Security Officer (CISO) merges the bank's Cyber Security strategy into its overarching Information Technology (IT) Policy to streamline documentation. What is the regulatory stance on this action?

(A) It is encouraged as it reduces documentation overhead for the Board and ensures administrative efficiency.
(B) It is permitted provided the bank classifies its riskiness as 'low' based on its current asset size.
(C) It is prohibited as the Cyber Security Policy must be distinct from the broader IT policy framework.
(D) It is acceptable only if the merged policy is reviewed by an independent external auditor for accuracy.

**Oct/Nov 2012**

**11.** What is the most appropriate step banks should take regarding cyber-security awareness among their Top Management and Board?

(A) Advise them to completely avoid using digital banking channels until all threats are neutralized.
(B) Delegate the responsibility of awareness and monitoring solely to the Board's IT Sub Committee.
(C) Ensure they only review summary-level incident reports annually during the general board meeting.
(D) Ensure they are brought up to speed on cyber-security aspects and organize appropriate familiarization.

**May/June 2007**

**12.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option:

Downloaded from www.pdf.tube

I Controls to protect data confidentiality
II Efficient and effective dispute resolution mechanism
III Swift corrective action via adequate review mechanisms
IV Availability of requisite infrastructure like human resources
V Permitting anonymous transactions up to a designated limit

Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (IV)
(B) (II), (III), (IV), and (V)
(C) (I), (II), (IV), and (V)
(D) (I), (III), (IV), and (V)

**Oct/Nov 2018**

**51.** Consider the following statements regarding the Application Security Life Cycle (ASLC):
I Regulated Entities (REs) must implement a multi-tier application architecture segregating application, database, and presentation layers.
II REs shall follow a 'secure by design' approach in development.
III Security can be retroactively applied after the product launch rather than embedded within the development lifecycle.

Which of the above statement(s) is/are correct?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) (I), (II), and (III)

**May/June 2024**

**52.** A bank suffers a major data breach. During the investigation, it is found that the Board of Directors never reviewed the cyber security infrastructure and failed to allocate adequate resources, ignoring the CISO's gap reports. Under the regulatory framework, what consequence applies to the board members?
(A) They are exonerated because the operational failure lies with the CISO and the internal IT department.
(B) They are required only to issue a public apology without any further financial or legal liability.
(C) Their liability is transferred to the third-party security vendor who managed the bank's firewalls.
(D) They are held directly liable due to their failure to establish due diligence in the risk review.

**Oct/Nov 2012**

**53.** Which of the following entities is NOT mandated to comply with the Master Directions on Digital Payment Security Controls?
(A) Payments Banks
(B) Small Finance Banks
(C) Regional Rural Banks
(D) Credit card issuing NBFCs

NODIA

**May/June 2007**

**54.** Conceptually, why is it mandated that web applications should not store sensitive information in HTML hidden fields, cookies, or any other client-side storage?
(A) To reduce the data storage costs on the bank's central servers
(B) To increase the processing speed of the web browser
(C) To avoid any compromise in the integrity of the data
(D) To bypass the need for multi-factor authentication

**Oct/Nov 2019**

**55.** Identify the incorrect statement regarding the Board/Senior Management's responsibilities.
(A) They shall review the policy at least once every three years.
(B) They must formulate a policy for digital payment products and services.
(C) They must ensure appropriate performance monitoring systems are in place.
(D) They are responsible for the implementation of the formulated policy.

**May/June 2014**

**56.** Identify the incorrect pair regarding the legal and regulatory framework:
(A) Sections 43, 43A - Payment Card Industry Data Security Standards (PCI-DSS)
(B) Regulator definition - Bank as data owner
(C) Bank Board liability - Held directly liable for lapses if due diligence is not established
(D) CISO - Chief Information Security Officer

**Oct/Nov 2005**

**57.** Match the items in List I with those in List II:
List I: (Cryptographic Elements)
P. Key length
Q. Algorithms
R. Digital certificates

# STUDYING FROM PDFs?

# THINK AGAIN.

If you are studying only from PDFs,
you are wasting valuable time.

Research shows that learning from

**PRINTED BOOKS** has up to

**4× HIGHER RETENTION**

than studying from screens.

**PRINT BOOK = BETTER MEMORY**

**PDF = LOWER RETENTION**

Those who study from **PRINTED BOOKS**
move **AHEAD.**

Others are left **BEHIND**
in competition.

In competitive exams,
being average is not enough.

## STAY ONE STEP AHEAD.

and risk of the bank.
(C) The policy must be identical for all banks to maintain a standardized defense against global cyber threats.
(D) Banks are required to submit the policy directly to ReBIT for final approval and compliance certification.

**Oct/Nov 2006**

**19.** Consider the following aspects that a Cyber Crisis Management Plan (CCMP) should explicitly address:
I Detection
II Mitigation
III Response
IV Recovery
V Containment
Which of the following combinations accurately reflects the four mandated aspects?
(A) (I), (II), (III), (V)
(B) (I), (III), (IV), (V)
(C) (II), (III), (IV), (V)
(D) (I), (II), (IV), (V)

**May/June 2009**

**20.** The IT Sub Committee of a bank's Board is reviewing an upgrade to its IT architecture. The proposed security measures entail significant financial costs, prompting the committee to consider a more affordable alternative that offers marginally less security. According to standard regulatory guidelines, how should the committee proceed?
(A) Record the risk and cost trade-off decisions in writing for future supervisory assessment.
(B) Adopt the affordable alternative without further documentation, as cost minimization is a board prerogative.
(C) Implement the costly measure immediately by bypassing the phased manner approach and budget constraints.
(D) Delegate the decision entirely to the third-party technology vendor to avoid organizational liability.

**Oct/Nov 2021**

**21.** A junior IT analyst in a bank detects a highly sophisticated remote access threat. Due to a flat organizational structure, the analyst struggles to bring the issue to the attention of decision-makers swiftly. Based on regulatory guidelines, what structural failure does this represent?
(A) Failure to independently audit the vulnerability assessment and patching process at the local level.
(B) Failure to implement biometric authentication for internal staff accessing the core banking systems.
(C) Failure to arrange for security concern escalation to appropriate levels for enabling quick action.
(D) Failure to formulate a distinct cyber security policy that addresses specific remote access threats.

**May/June 2019**

**22.** Consider the following statements regarding the initial guidelines on Information Security and Cyber Frauds:
I The guidelines were provided by the G. Gopalakrishna Committee vide a circular dated April 29, 2011.
II The measures suggested for implementation were indicated to be static to ensure uniform compliance across all banks.
Which of the above statement(s) is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**Oct/Nov 2010**

**23.** Match the items in List I with those in List II:
List I: (Inherent Risk Categorizations)
P. Low
Q. Moderate
R. High
S. Very High
List II: (Appropriateness)
1. Baseline risk category necessitating standard preventive controls
2. Elevated risk category requiring advanced monitoring capabilities
3. Severe risk category necessitating highly adaptive incident response
4. Moderate risk category requiring periodic vulnerability testing
(A) P-2, Q-3, R-1, S-4
(B) P-1, Q-4, R-2, S-3
(C) P-3, Q-1, R-4, S-2
(D) P-4, Q-2, R-3, S-1

Click Here to Buy book on Amazon

May/June 2020

**24.** Consider the following statements about measuring cyber security preparedness:

I Adequacy of the cyber resilience framework should be assessed through the development of indicators.

II Indicators should be used for comprehensive testing through independent compliance checks and audits.

III Audits must be carried out exclusively by the bank's internal IT staff.

IV Awareness among stakeholders, including employees, may form a part of this assessment.

V The assessment aims to measure the level of risk/preparedness.

Which of the above statement(s) is/are correct?

(A) (I), (II), IV), and (V)
(B) (I), (III), (IV), and (V)
(C) (II), (III), (IV), and (V)
(D) (I), (II), (III), and (IV)

Oct/Nov 2024

**25.** Identify the correct pair concerning the protection of customer information:

(A) Custodial information - Confidentiality should be compromised only during transit with third-party vendors
(B) Data lifecycle - Suitable systems and processes need to be put in place by banks
(C) Bank's role - Acts merely as an 'intermediary' under the IT Act
(D) Data storage - Integrity is required only when data is stored within the bank itself

May/June 2005

**26.** Why does the traditional information security framework fail to adequately cover emerging risks in the modern digitized banking landscape?

(A) It predominantly focuses on external physical threats and legacy perimeter defenses rather than digital vulnerabilities.
(B) It relies exclusively on hardware encryption mechanisms which are now largely obsolete in modern banking.
(C) It does not mandate the use of multi-factor authentication for core banking operations across all platforms.
(D) It has limited coverage of risks like cyber warfare, Internet of Things (IoT), and modern social trolling.

Oct/Nov 2011

**27.** The Indian Banks – Center for Analysis of Risks and Threats (IB-CART) was set up by which organization?

(A) IDRBT
(B) CERT-In
(C) ReBIT
(D) NCIIPC

May/June 2017

**28.** When identifying and assessing inherent risks to adopt an appropriate cyber-security framework, banks are required to consider multiple factors. Which of the following is NOT explicitly mentioned as a factor to be considered?

(A) Profitability of the delivery channels
(B) Technologies adopted
(C) Alignment with business and regulatory requirements
(D) Organizational culture and internal & external threats

Oct/Nov 2020

**29.** Which of the following is NOT listed as a cyber-threat that banks should be prepared to face and address through their CCMP?

(A) Distributed denial of services (DDoS)
(B) Ransomware / cryptoware
(C) Cross-site scripting vulnerabilities in non-financial public forums
(D) Spear phishing and whaling

May/June 2025

**30.** What is the fundamental conceptual role of a Security Operations Centre (SOC) as envisaged in regulatory guidelines?

(A) To process and authorize high-value financial transactions securely
(B) To develop commercial digital payment applications
(C) To act as a data repository for customer grievance redressal
(D) To continuously monitor and manage cyber risks in real time

Oct/Nov 2015

**31.** Which of the following is NOT highlighted as a key prescription in standard cyber security frameworks for banks?

(A) Addressing network and database security comprehensively to prevent unauthorized access and data theft.
(B) Formulating an adaptive Cyber Crisis

NODIA

Management Plan (CCMP) to address detection and recovery.
(C) Outsourcing all cyber risk management tasks to the Computer Emergency Response Team - India (CERT-In).
(D) Ensuring confidentiality, integrity, and availability of custodial information across all bank systems.

**May/June 2006**

**32.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option:
Assertion (A): Whenever Regulated Entities (REs) are dependent on third party service providers, they must implement adequate oversight and controls for monitoring third party personnel.
Reason (R): Third party service providers fall outside the regulatory purview and thus absolve REs of data confidentiality breaches.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2022**

**33.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option:
Assertion (A): Banks cannot avoid liability under sections 43, 43A of the IT Act 2000/2008 by defining themselves merely as 'intermediaries'.
Reason (R): Since a bank is defined as the data owner, it is the bank's duty and responsibility to protect the confidentiality, integrity, and availability of data.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2012**

**34.** What is the most appropriate technological mitigation mandated to secure digital payment products and services offered over the Internet against overwhelming traffic attacks?
(A) Full Hard Disk Encryption (FHDE)
(B) Distributed Denial of Service (DDoS) mitigation techniques
(C) Virtual Private Network (VPN) exclusively for customers
(D) Device binding via IMEI number

**Oct/Nov 2016**

**35.** By what term are the institutions governed by the Master Directions on Digital Payment Security Controls collectively referred?
(A) Regulated Entities (REs)
(B) Governed Financial Institutions (GFIs)
(C) Authorized Payment Enablers (APEs)
(D) Chartered Banking Organizations (CBOs)

**May/June 2023**

**36.** A Regulated Entity (RE) partners with a fintech startup to co-develop a new digital wallet. During the Application Security Life Cycle (ASLC), the developers bypass threat modelling to speed up the rollout. Does this action comply with directives?
(A) No, REs partnering to co-develop applications must incorporate a threat modelling approach.
(B) Yes, threat modelling is only required for legacy core banking systems and not for new wallets.
(C) Yes, provided the fintech startup assumes all financial liability in writing for potential leaks.
(D) No, because co-branding with fintech startups is strictly prohibited under current banking laws.

**Oct/Nov 2008**

**37.** Identify the correct statement regarding stakeholder awareness in the context of cyber-security.
(A) If the bank fails to create awareness, the stakeholder is not held responsible for resulting incidents.
(B) Stakeholders include only the employees and internal partners directly involved in the bank's IT systems.
(C) The bank must ensure that stakeholders are

Downloaded from www.pdf.tube

Assertion (A): Traditional information security issues and emerging threats from cyberspace need to be covered under a single unified Information Security framework.
Reason (R): The emerging technologies and tools within cyberspace rapidly increase organizational exposure to new vulnerabilities.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2019**

**13.** What defines a Cyber Crisis Management Plan (CCMP)?
(A) A Board-approved strategy addressing Detection, Response, Recovery, and Containment of cyber-risks.
(B) A traditional Business Continuity Plan solely focused on natural disasters and physical infrastructure.
(C) An isolated technical manual utilized exclusively by the SOC team for internal maintenance tasks.
(D) A regulatory filing submitted annually to the CSITE Cell detailing financial losses from cyber frauds.

**May/June 2014**

**14.** Which of the following statements is incorrect concerning the arrangement for continuous surveillance in banks?
(A) Testing for vulnerabilities at reasonable intervals of time is deemed very important.
(B) Setting up a Security Operations Centre (SOC) is mandated at the earliest.
(C) Cyber-attacks are predictable and generally follow patterns that can be fully anticipated.
(D) The SOC must ensure continuous surveillance and keep regularly updated on emerging threats.

**Oct/Nov 2005**

**15.** Which of the following statements is incorrect regarding the reporting of cyber-security incidents?
(A) Banks need to report all unusual cyber-security incidents.
(B) Attempts of cyber-incidents which did not fructify must also be reported.
(C) All cyber security incidents must be reported to the regulator within 2 to 6 hours.
(D) Only successful cyber-attacks that result in financial loss need to be reported.

**May/June 2022**

**16.** What is the definition of Cyberspace in the context of Cyber Security?
(A) Interconnected networks of information systems, infrastructures, the Internet, and computer systems.
(B) A localized environment designed solely for secure banking transactions and encrypted financial data.
(C) An isolated intranet facilitating internal communication within a bank and its branches.
(D) A regulatory sandbox environment for testing new digital payment applications and system logic.

NODIA

**Oct/Nov 2017**

**17.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option:
Assertion (A): Collaboration among entities in sharing cyber-incidents and best practices is discouraged as it risks exposing a bank's vulnerabilities.
Reason (R): Banks are historically hesitant to share cyber-incidents faced by them.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2013**

**18.** Which of the following statements is correct regarding the implementation of the Cyber-security Policy by banks?
(A) Banks should immediately implement a Board-approved cyber-security policy and strategy.
(B) Banks must formulate a policy but board approval is optional depending on the size

transaction volumes and successful cross-selling of apps.
(D) To track the profitability of third-party outsourcing contracts for infrastructure and maintenance.

**May/June 2018**

**44.** Consider the following statements regarding the policy for digital payment products, which should explicitly discuss requirements from the Functionality, Security, and Performance (FSP) angles:
I Assurance that the payment product is built in a secure manner
II Capacity building and expansion with scalability
III Minimal customer service disruption with high availability
IV Mandatory physical branch visits for initial activation
Which of the above statement(s) is/are correct?
(A) (I), (II), and (IV)
(B) (I), (III), and (IV)
(C) (II), (III), and (IV)
(D) (I), (II), and (III)

**Oct/Nov 2014**

**45.** Identify the correct statement regarding digital certificates and application monitoring.
(A) Mobile applications are exempt from logging user activity if internet banking handles the monitoring.
(B) The key length for asymmetric encryption should be customized locally rather than adopting internationally accepted standards.
(C) Digital certificates used in the digital payment ecosystem must be renewed well in time.
(D) Effective monitoring is only required to track security changes, not anomalous transactions.

**May/June 2021**

**46.** Consider the following aspects that a Cyber Crisis Management Plan (CCMP) should explicitly address:
I Detection
II Mitigation
III Response
IV Recovery
V Containment
Which of the following combinations accurately reflects the four mandated aspects?
(A) (I), (II), (III), (V)
(B) (I), (III), (IV), (V)
(C) (II), (III), (IV), (V)
(D) (I), (II), (IV), (V)

**Oct/Nov 2009**

**47.** Which of the following is an exception to the mandated generic security controls for digital payment channels?
(A) Adhering to secure standard communication protocols over the Internet
(B) Storing unencrypted customer passwords in client-side cookies for session continuity
(C) Implementing an appropriate level of encryption
(D) Implementing Web Application Firewall (WAF) solutions

**May/June 2016**

**48.** According to regulatory highlights, within what time frame must all cyber security incidents be reported to the regulator?
(A) Within 1 to 3 hours
(B) Within 2 to 6 hours
(C) Within 12 to 24 hours
(D) Within 48 hours

**Oct/Nov 2023**

**49.** A Small Finance Bank is launching a new mobile banking app. Before offering the service, the IT department decides to skip the evaluation of client-side application architecture risks to meet an aggressive launch deadline. Based on guidelines, what critical failure has occurred?
(A) Failure to evaluate technology platform risks on both the server side and the client side.
(B) Failure to notify the regulator within 2 to 6 hours of the product launch and marketing campaign.
(C) Failure to execute a physical vulnerability assessment of the bank's branches and storage facilities.
(D) Failure to mandate biometric authentication for all users regardless of their device capabilities.

**May/June 2011**

**50.** Consider the following aspects that must be ensured to meet the FSP angles for digital payment products:

Click Here to Buy book on Amazon

kept unaware of potential impacts to avoid widespread panic.
(D) Awareness programs and educational campaigns are exclusively the responsibility of third-party vendors.

**May/June 2010**

**38.** Match the items in List I with those in List II:
List I: (Operational Requirements)
P. Capacity building
Q. High availability of systems
R. Dispute resolution mechanism
S. Robust architecture
List II: (Descriptive Goals)
1. To meet the growth for efficient transaction processing
2. To have minimal technical declines
3. Handling of customer grievance effectively
4. Commensurate with transaction volumes and customer growth
(A) P-1, Q-2, R-3, S-4
(B) P-2, Q-3, R-4, S-1
(C) P-4, Q-1, R-2, S-3
(D) P-3, Q-4, R-1, S-2

**Oct/Nov 2013**

**39.** What is the mandated minimum frequency for testing backed-up data and applications pertaining to digital products to ensure recovery without loss?
(A) Weekly
(B) Monthly
(C) Half-yearly
(D) Yearly

**May/June 2008**

**40.** Arrange the following events regarding regulatory guidelines on cyber security in chronological order:
I Notification of the Cyber Security Framework for Banks offering significant benefits
II First issuance of Cyber Security Guidelines by the regulator
III Revision of guidelines based on recommendations of the G Gopalakrishna Committee
IV Required deadline for CISO to report gaps and come up with a viable plan
(A) (I), (II), (IV), (III)
(B) (II), (III), (I), (IV)
(C) (III), (II), (I), (IV)
(D) (II), (I), (III), (IV)

**Oct/Nov 2007**

**41.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option:
Assertion (A): Regulated Entities (REs) must have an escrow arrangement for the source-code of digital payment applications licensed by a third-party vendor.
Reason (R): This arrangement ensures the continuity of services in case the vendor defaults or is unable to provide services.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2015**

**42.** Identify the correct statement regarding the liability of board members concerning cyber security:
(A) Board members are entirely shielded from direct liability for cyber lapses by the appointment of a CISO.
(B) Board liability is strictly limited to financial misreporting and does not cover operational cyber losses.
(C) Board members can be held liable if they fail to establish due diligence in addressing cyber security.
(D) Liability only arises if the board explicitly authorizes a malicious cyber-attack on a competing entity.

**Oct/Nov 2025**

**43.** What is the primary conceptual purpose of establishing Key Performance Indicators (KPIs) and performance monitoring systems by the Board/Senior Management?
(A) To evaluate the marketing success of new digital products and the growth of the customer user base.
(B) To assess whether digital payment services meet the required operational and security standards.
(C) To determine employee bonuses based on

NODIA

S. Logging and monitoring

List II: (Functions or Usage)

1. Used for encryption, signing, and creation of message digest
2. Must be renewed well in time in the payment ecosystem
3. Applies to symmetric/asymmetric encryption and hashing to ensure strong security
4. Tracks user activity and identifies anomalous behaviour in applications

(A) P-3, Q-1, R-2, S-4
(B) P-1, Q-3, R-4, S-2
(C) P-4, Q-2, R-1, S-3
(D) P-2, Q-4, R-3, S-1

**May/June 2022**

**58.** A newly licensed Regional Rural Bank (RRB) is designing its digital payment architecture. The management decides not to adhere to the Master Directions on Digital Payment Security Controls, claiming an exemption. Is their interpretation correct based on the applicability criteria?

(A) Yes, because Scheduled Commercial Banks excluding RRBs are specified under the applicability clause.
(B) No, because all banks operating in India must follow the Master Directions regardless of their size.
(C) No, because RRBs fall under the category of Small Finance Banks which are mandated to follow it.
(D) Yes, but only if they do not offer Internet banking services and stick to traditional branch banking.

**Oct/Nov 2017**

**59.** Consider the following statements regarding capacity management and data recovery:

I Regulated Entities (REs) must periodically test backed-up data to ensure recovery without loss of transactions or audit-trails.
II These facilities should be tested at least on a quarterly basis for digital payment products and services.

Which of the above statement(s) is/are correct?

(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**May/June 2013**

**60.** Identify the correct statement regarding the Governance and Management of Security Risks.

(A) The policy for digital payment products and services requires approval solely from the bank's CISO.
(B) The Board and Senior Management are responsible for implementation and must review the policy yearly.
(C) The Board and Senior Management shall review the policy periodically, at least on a half-yearly basis.
(D) Third-party service providers are exempt from regulator guidelines on outsourcing of payment services.

**Oct/Nov 2006**

**61.** A customer is attempting a high-value fund transfer from an unfamiliar international location. The bank's system temporarily pauses the transaction and requests a secondary OTP. Which directive validates this automated system behavior?

(A) The mandate to execute Code Obfuscation on the server
(B) The requirement to renew digital certificates in time
(C) The adoption of Adaptive Authentication factors depending on user risk profile and behaviour
(D) The escrow arrangement for source code

**May/June 2009**

**62.** Conceptually, why should the appearance, look, and feel of a Regulated Entity's (RE) internet banking site be made uniform when accessed through external websites like e-commerce or tax portals?

(A) To ensure customers recognize legitimate interfaces and mitigate phishing risks during authentication.
(B) To minimize the graphic design expenses for the bank and the third-party web application vendors.
(C) To bypass the WAF solutions implemented by the external websites for faster transaction processing.
(D) To allow external vendors to collect the customer's login credentials for secondary marketing use.

NQDIA

**Oct/Nov 2021**

**63.** Before launching a new UPI-based payment service, a bank performs an extensive review of its marketing strategy but ignores testing the functionality against functional requirements and specifications. According to security requirements, what mandatory step was missed?

(A) Thoroughly testing functionality and security controls before moving to the production environment.
(B) Outsourcing the server hosting to a foreign jurisdiction to ensure data redundancy and safety.
(C) Providing source code to all retail customers for open-source review and bug bounty participation.
(D) Ensuring the application stores unencrypted passwords for faster login and better user experience.

**May/June 2019**

**64.** What is the most appropriate practice mandated regarding the storage of customer data by a mobile application?

(A) The application should permanently store user IDs and passwords to improve user convenience and speed.
(B) Sensitive information should be written to the database in plain text to allow rapid system retrieval.
(C) Securely wipe sensitive customer information from memory when the user exits the mobile application.
(D) Hard coded references must be retained on the device to speed up authentication and data processing.

**Oct/Nov 2010**

**65.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option:

Assertion (A): Regulated Entities (REs) must implement a real time/near-real time reconciliation framework for all digital payment transactions.

Reason (R): Timely reconciliation (not later than 24 hours from the receipt of settlement files) facilitates better detection and prevention of suspicious transactions.

(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2020**

**66.** Identify the incorrect statement regarding the security of mobile applications.

(A) Web content must be loaded even if errors are detected during SSL/TLS negotiation to ensure speed.
(B) Device binding of the mobile application shall be ensured for all active user accounts and logins.
(C) The checksum of the current active version shall be hosted on a public platform for user verification.
(D) The app should require re-authentication whenever the device remains unused for a designated period.

**Oct/Nov 2024**

**67.** Identify the correct pair regarding the mandatory frequency of security testing for digital payment applications:

(A) Vulnerability Assessment (VA) - Conducted at least on a quarterly basis
(B) Penetration Testing (PT) - Conducted at least on a yearly basis
(C) Vulnerability Assessment (VA) - Conducted at least on a half-yearly basis
(D) Penetration Testing (PT) - Conducted only when a breach occurs

**May/June 2005**

**68.** A bank introduces a new biometric authentication feature for its mobile app. However, it fails to provide any instructions or communication to the customers on how to utilize it, leading to a surge in locked accounts. What regulatory expectation did the bank violate?

(A) The mandate to notify the regulator before adding any biometric feature to the mobile banking app.
(B) The requirement that clear communication and instructions be provided when new security features are added.
(C) The rule preventing the use of biometrics for digital payments to protect user privacy

Downloaded from www.pdf.tube

and data.

(D) The mandate to physically demonstrate the feature at home branches to every active account holder.

**Oct/Nov 2011**

**69.** Which of the following is NOT a mandated control for mobile payment applications?

(A) Maintaining all historical versions to ensure backward compatibility across all legacy devices.

(B) Application secure download and install procedures to prevent the injection of malicious code.

(C) Device or application encryption to protect sensitive data stored on the physical hardware.

(D) Ensuring minimal data collection and specific app permissions for improved customer privacy.

**May/June 2017**

**70.** Which of the following is NOT listed as a required skill or area of expertise for staff in the fraud control function?

(A) Investigative techniques and procedures

(B) Cardholder and merchant education techniques to prevent fraud

(C) Advanced software programming for developing proprietary operating systems

(D) Liaising or communicating with law enforcement agencies

**Oct/Nov 2020**

**71.** Match the items in List I with those in List II:

List I: (Master Direction Requirements)

P. WAF implementation

Q. PCI-DSS compliance

R. CCMP formulation

S. Re-authentication

List II: (Corresponding Actions)

1. Ensuring payment card data security
2. Defending web applications against online threats
3. Required when a mobile app remains unused for a designated period
4. Addressing detection, response, recovery, and containment

(A) P-2, Q-1, R-4, S-3

(B) P-1, Q-2, R-3, S-4

(C) P-4, Q-3, R-2, S-1

(D) P-3, Q-4, R-1, S-2

**May/June 2025**

**72.** What is the conceptual reason behind the mandate to redact or mask customer information such as account numbers and card numbers when transmitted via SMS or e-mails?

(A) To compress the size of the SMS to reduce telecom charges and ensure rapid delivery to the user.

(B) To protect sensitive payment data from exposure and potential misuse during the transmission process.

(C) To comply with advertising standard limitations on message character counts for marketing texts.

(D) To ensure the customer memorizes their complete account details for all future manual transactions.

**Oct/Nov 2015**

**73.** Identify the incorrect statement regarding Internet Banking Security Controls.

(A) An online session shall be automatically terminated after a fixed period of inactivity.

(B) Authentication procedures should be uniform when accessed through external websites.

(C) Applications are vulnerable to application layer Denial of Service (DoS) attacks.

(D) Passwords generated and dispatched by the Regulated Entity (RE) must possess unlimited validity.

**May/June 2006**

**74.** Consider the following statements regarding Customer Protection and Awareness:

I Regulated Entities (REs) shall adhere to extant instructions to put in place systems for online dispute resolution.

II Customers shall be educated to download applications from any available third-party website to ensure maximum accessibility.

Which of the above statement(s) is/are correct?

(A) Only (I)

(B) Only (II)

(C) Both (I) and (II)

(D) Neither (I) nor (II)

**Oct/Nov 2022**

**75.** A bank utilizes SMS-based OTP for authenticating mobile banking transactions. Given that the mobile application and the

NODIA

authentication factor (SMS) reside on the same device, which of the following actions is advised?
(A) Disabling OTP completely for mobile banking transactions.
(B) Issuing a secondary smartphone to all customers exclusively for receiving OTPs.
(C) Switching entirely to email-based OTPs, removing mobile apps.
(D) Implementing alternatives to SMS-based OTP authentication mechanisms.

**May/June 2012**

**76.** Consider the following conditions and identify which necessitate conducting Vulnerability Assessment (VA) and Penetration Testing (PT) outside of their regular scheduled intervals:
I When a new IT Infrastructure is introduced
II When a new digital payment application is introduced
III When a minor cosmetic update is made to the website frontend
IV When any major change is performed in the application or infrastructure
Which of the above statement(s) is/are correct?
(A) (I), (II), and (IV)
(B) (II), (III), and (IV)
(C) (I), (III), and (IV)
(D) (I), (II), and (III)

**Oct/Nov 2016**

**77.** Identify the correct statement regarding the maintenance of mobile application versions by a Regulated Entity (RE).
(A) The RE must maintain at least three active versions to support older and legacy smartphones.
(B) REs are prohibited from verifying the version of the mobile application before enabling transactions.
(C) The phase-out period applies exclusively to iOS applications and not to the Android ecosystem.
(D) Deactivate older versions within six months of the release of a newer version in a timely manner.

**May/June 2023**

**78.** What is the most appropriate action a Regulated Entity (RE) must take regarding failed log-in attempts on a digital payment service?
(A) Block the user indefinitely and require the creation of a new bank account at a physical branch.
(B) Allow unlimited attempts but throttle the processing speed after 5 attempts to deter bot scripts.
(C) Automatically deduct a penalty fee from the user's account after 3 failed attempts as a deterrent.
(D) Block access after a set number of attempts, notify the customer, and use a secure re-activation process.

**Oct/Nov 2008**

**79.** While using a mobile payment application, a customer's device detects an anomaly for which the application was not programmed. According to directives on Mobile Payments Application Security Controls, what is the expected immediate outcome?
(A) The app silently patches itself in the background without user intervention or any external notice.
(B) Direct the customer to remove the current application and proceed with the installation of a new copy.
(C) The bank immediately freezes all funds in the user's account for 30 days to investigate the anomaly.
(D) The app downgrades to the oldest available version to restore basic functionality for the user.

**May/June 2010**

**80.** Identify the incorrect pair regarding what customers should be educated about for the physical and logical security of their devices:
(A) App sources - Downloading applications only from authorised sources
(B) Updates - Secure/regular installation of operating system and application updates
(C) Security tools - Having anti-malware/anti-virus applications on devices
(D) Connectivity - Connecting exclusively via public open Wi-Fi for all financial transactions

**Oct/Nov 2013**

**81.** Conceptually, what is the significance of displaying certificate errors (e.g., expiry, revocation, or unrecognised authority) to the user during an SSL/TLS negotiation?
(A) To inform the user that their internet connection is too slow for secure banking

Click Here to Buy book on Amazon

transactions.
(B) To prompt the user to update their mobile operating system to the latest version immediately.
(C) To warn of potential Man-in-the-Middle attacks or insecure connections, preventing compromised data.
(D) To advertise the bank's preferred security vendor and digital certificate provider to the customer.

**May/June 2008**

**82.** Which definition accurately describes "Adaptive Authentication"?
(A) A method to send notifications or prompt consumers to complete additional steps to verify identities when requests are deemed doubtful
(B) A biometric scan strictly enforced for all mobile app logins irrespective of transaction size
(C) A physical security token that changes its encryption key every 24 hours
(D) An authentication protocol that adapts offline passwords to internet banking sessions

**Oct/Nov 2007**

**83.** Match the items in List I with those in List II:
List I: (Fraud Risk Management Elements)
P. Suspicious transactional behaviour
Q. System alerts
R. Fraud analysis
S. False positives
List II: (Regulatory Requirements)
1. Must be parameterized and monitored in terms of various applicable parameters
2. Identified through documented rules and detective controls
3. Fraud control staff must differentiate these from actual threats
4. Conducted to identify reasons for occurrence and determine preventive mechanisms
(A) P-1, Q-2, R-3, S-4
(B) P-2, Q-1, R-4, S-3
(C) P-4, Q-3, R-1, S-2
(D) P-3, Q-4, R-2, S-1

**May/June 2015**

**84.** Match the items in List I with those in List II:
List I: (Mobile App Security Controls)
P. Code obfuscation
Q. Sandboxing
R. Remote access identification
S. Phase-out mechanism
List II: (Functional Descriptions)
1. Deactivating older app versions within a maximum of six months
2. Isolating the application environment to protect it from other device apps
3. Prohibiting login access if screen-sharing or remote control apps are detected
4. Modifying the source code to make it difficult for attackers to reverse engineer
(A) P-4, Q-2, R-3, S-1
(B) P-1, Q-3, R-2, S-4
(C) P-2, Q-4, R-1, S-3
(D) P-3, Q-1, R-4, S-2

**Oct/Nov 2025**

**85.** Consider the following statements regarding Internet Banking Security Controls:
I Internet banking websites are vulnerable to authentication related brute force attacks.
II An online session can remain active indefinitely as long as the web browser is open.
III Secure delivery of password for login purpose shall be ensured and should be valid for a limited period.
Which of the above statement(s) is/are correct?
(A) Only (I) and (II)
(B) Only (II) and (III)
(C) Only (I) and (III)
(D) (I), (II), and (III)

**May/June 2018**

**86.** Identify the incorrect statement regarding the handling of unauthorized payment products and data transmission.
(A) A mechanism shall be instituted to actively monitor for non-genuine applications on popular app-stores.
(B) Regulated Entities (REs) shall transmit complete, unredacted customer account numbers via SMS to ensure transparency.
(C) The server should have checks to ensure no transaction is carried out through unauthorized digital payment applications.
(D) The authentication process must be robust, secure, and centralised.

NODIA

S. Validating against PCI-P2PE

List II: (Intended Protections)

1. Prevents unauthorized extraction of card magnetic stripe data at the machine
2. Protects card details via point-to-point encryption at merchant terminals
3. Restricts maintenance privileges to specific approved windows, reducing insider threats
4. Prevents the execution of unauthorized malicious software via external hardware

(A) P-4, Q-1, R-3, S-2
(B) P-1, Q-4, R-2, S-3
(C) P-3, Q-2, R-1, S-4
(D) P-2, Q-3, R-4, S-1

**May/June 2022**

**100.** A Scheduled Commercial Bank is developing a new UPI application. During the design phase, the product manager focuses exclusively on offering robust performance and high availability to ensure minimal technical declines. However, they allocate no resources for data encryption. Which of the 'FSP angles' has the product manager neglected?
(A) Functionality
(B) Performance
(C) Security
(D) Scalability

**Oct/Nov 2017**

**101.** A small payment bank argues that due to a lack of skilled manpower, it cannot set up a SOC and will instead rely on quarterly reviews by a third-party consultant. Does this meet regulatory guidelines?
(A) No, banks must set up and operationalize a SOC to monitor cyber risks and threats in real time.
(B) Yes, third-party consultants fulfill the continuous surveillance requirement through periodic audits.
(C) Yes, payment banks are exempt from setting up a SOC due to their specialized and limited license.
(D) No, the SOC must be managed entirely by the IT subsidiary to maintain complete internal control.

**May/June 2013**

**102.** Consider the following statements regarding the overarching principles of digital payment security:

I Master directions are issued chiefly from the perspective of customer protection amidst the explosive proliferation of digital payments.

II Master directions serve merely as an optional guiding tool and are not mandatory for Regulated Entities.

Which of the above statement(s) is/are correct?
(A) Only (I)
(B) Only (II)
(C) Both (I) and (II)
(D) Neither (I) nor (II)

**Oct/Nov 2006**

**103.** An aggregator processes thousands of digital transactions daily. A dispute arises over a mismatch in settlement files. Under the reconciliation framework, what is the maximum permissible delay before the bank must reconcile these transaction files?
(A) 12 hours
(B) 24 hours
(C) 48 hours
(D) 7 days

**May/June 2009**

**104.** Conceptually, which term refers to the interconnected network of information systems or infrastructures such as the Internet, telecommunications networks, and embedded processors?
(A) Sandbox environment
(B) Extranet
(C) Dark web
(D) Cyberspace

**Oct/Nov 2021**

**105.** Match the items in List I with those in List II:

List I: (Terms)

P. WAF
Q. BYOD
R. DDoS
S. PCI-DSS

List II: (Keyword Definitions)

1. Payment Card Industry-Data Security Standards
2. Bring Your Own Device
3. Distributed Denial of Service
4. Web Application Firewall

(A) P-4, Q-2, R-3, S-1
(B) P-2, Q-1, R-4, S-3
(C) P-1, Q-3, R-2, S-4

Downloaded from www.pdf.tube

of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2018**

**93.** Identify the correct statement regarding ATM operating systems.
(A) Banks are permitted to run unsupported operating systems if they disable internet access on the ATM.
(B) Operating systems on ATMs only need to be patched once every five years.
(C) Use of ATMs that have unsupported operating systems shall be prohibited.
(D) ATMs must run entirely on open-source Linux distributions without exception.

**May/June 2024**

**94.** A hacker utilizes automated software to guess a user's internet banking password by systematically trying thousands of combinations. What mandatory control should the bank have in place to thwart this specific attack?
(A) Application containerization
(B) An escrow arrangement for source code
(C) A maximum number of failed log-in attempts set down after which access is blocked
(D) Mandatory biometric attendance for bank staff

**Oct/Nov 2012**

**95.** Identify the incorrect statement regarding the functions or nature of ReBIT.
(A) ReBIT stands for Reserve Bank Information Technology Pvt. Ltd.
(B) It caters solely to the cyber security needs of foreign banks operating outside India.
(C) It is an IT subsidiary created by the Reserve Bank of India.
(D) Its purpose includes ensuring the cyber resilience of Indian banking.

**May/June 2007**

**96.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option:
Assertion (A): The CISO of a bank had to report gaps between the actual state of affairs and the new cyber security requirement by July 2016.
Reason (R): This reporting forced banks to provide more resources to address cyber security and come up with a viable remediation plan.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**Oct/Nov 2019**

**97.** Consider the following measures and identify which are mandated to improve the security posture of ATMs:
I Implementing BIOS passwords
II Disabling USB ports and auto-run facility
III Implementing anti-skimming and whitelisting solutions
IV Upgrading ATMs with supported versions of operating systems
V Allowing time-based admin access
Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (IV)
(B) (II), (III), (IV), and (V)
(C) (I), (II), (IV), and (V)
(D) (I), (II), (III), (IV), and (V)

**May/June 2014**

**98.** Identify the correct statement regarding customer communication for unauthorized transactions.
(A) Regulated Entities should provide a mechanism on their app for customers to mark transactions as fraudulent.
(B) Customers must visit a branch physically to report an unauthorized mobile transaction to the manager.
(C) REs have up to 72 hours to acknowledge a fraudulent transaction marking from a verified user account.
(D) Customers are not allowed to mark transactions as fraudulent if they used a PIN for the transaction.

**Oct/Nov 2005**

**99.** Match the items in List I with those in List II:
List I: (ATM and Card Payment Security Measures)
P. Disabling USB ports
Q. Anti-skimming solutions
R. Time-based admin access

NODIA

availability of data
II To ensure the bank defines itself purely as an intermediary
III To create cyber security awareness among all stakeholders
Which of the above statement(s) is/are correct?
(A) Only (I) and (II)
(B) Only (I) and (III)
(C) Only (II) and (III)
(D) (I), (II), and (III)

**Oct/Nov 2020**

**113.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option:
Assertion (A): For digital payment applications licensed by a third party, Regulated Entities (REs) must have an escrow arrangement for the source-code.
Reason (R): The escrow arrangement guarantees that the third party will continuously update the source code with new features.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

**May/June 2025**

**114.** What is the most appropriate purpose of Code Obfuscation in a mobile payment application?
(A) To compress the application file size for faster download and installation on devices with low memory.
(B) To make the application's source code difficult for attackers to understand and reverse engineer.
(C) To enhance the graphical user interface and ensure compatibility for older and legacy mobile devices.
(D) To bypass the Apple or Google App Store review process and ensure rapid deployment of new features.

**Oct/Nov 2015**

**115.** Which of the following is NOT required for improving ATM security posture?
(A) Disabling the auto-run facility
(B) Applying the latest patches of the operating system
(C) Installing unsupported operating systems to obscure source code
(D) Implementing terminal security solutions

**May/June 2006**

**116.** Which of the following is an exception to the mandated requirements for robust surveillance and monitoring of card transactions?
(A) Monitoring overseas cash withdrawals closely
(B) Setting up rules and limits commensurate with the Regulated Entity's (RE) risk appetite
(C) Identifying unencrypted (clear text) payment card data in the ecosystem to adhere to safety measures
(D) Disabling transaction limits at the Card and BIN level to ensure customer convenience

**Oct/Nov 2022**

**117.** Identify the incorrect statement regarding the customer grievance mechanism.
(A) A section specifying the process and procedure to lodge grievances must be incorporated into the app.
(B) The grievance section should include forms and contact information.
(C) Regulated Entities (REs) must adhere to extant instructions for resolving disputes pertaining to digital payments.
(D) Online Dispute Resolution (ODR) systems are prohibited due to security concerns.

**May/June 2012**

**118.** Match the items in List I with those in List II:
List I: (Master Direction Requirements)
P. WAF implementation
Q. PCI-DSS compliance
R. CCMP formulation
S. Re-authentication
List II: (Corresponding Actions)
1. Ensuring payment card data security
2. Defending web applications against online threats
3. Required when a mobile app remains unused for a designated period
4. Addressing detection, response, recovery, and containment
(A) P-2, Q-1, R-4, S-3
(B) P-1, Q-2, R-3, S-4

Click Here to Buy book on Amazon

(D) P-3, Q-4, R-1, S-2

May/June 2019

**106.** Match the items in List I with those in List II:

List I: (ATM and Card Payment Security Measures)

P. Disabling USB ports
Q. Anti-skimming solutions
R. Time-based admin access
S. Validating against PCI-P2PE

List II: (Intended Protections)

1. Prevents unauthorized extraction of card magnetic stripe data at the machine
2. Protects card details via point-to-point encryption at merchant terminals
3. Restricts maintenance privileges to specific approved windows, reducing insider threats
4. Prevents the execution of unauthorized malicious software via external hardware

(A) P-4, Q-1, R-3, S-2
(B) P-1, Q-4, R-2, S-3
(C) P-3, Q-2, R-1, S-4
(D) P-2, Q-3, R-4, S-1

Oct/Nov 2010

**107.** Conceptually, why does Adaptive Authentication prompt the consumer to complete an additional verification step?

(A) Because the authentication request is deemed doubtful according to the security policy and risk assessment.
(B) Because the consumer's internet bandwidth is detected as low for processing secure financial data.
(C) Because the bank wishes to test the speed and reliability of the global OTP delivery network.
(D) Because a minimum of three verification steps is mandated for every login into the mobile app.

May/June 2020

**108.** Consider the following acronyms and identify which are correctly defined:

I BYOD - Bring Your Own Device
II FHDE - Full Hard Disk Encryption
III VAPT - Vulnerability Assessment and Penetration Testing
IV OEM - Original Equipment Manufacturer
V CISO - Chief Information Security Officer

Which of the above statement(s) is/are correct?

(A) (I), (II), (III), and (V)
(B) (II), (III), (IV), and (V)
(C) (I), (III), (IV), and (V)
(D) (I), (II), (III), (IV), and (V)

Oct/Nov 2024

**109.** Identify the incorrect statement concerning Application Security Life Cycle (ASLC).

(A) Regulated Entities (REs) shall implement a multi-tier application architecture for better data isolation.
(B) REs must follow a 'secure by design' approach during the initial development and coding phases.
(C) Security must be embedded within the development lifecycle rather than being added after the launch.
(D) Presentation and database layers can be combined into a single layer to enhance transaction speed.

May/June 2005

**110.** What is the most appropriate description of a 'Zero-day' attack as contextually inferred from the requirements of a CCMP?

(A) An attack executed exactly at midnight
(B) A traditional banking fraud involving physical theft
(C) An emerging, unanticipated cyber-threat for which no patch currently exists
(D) An attack that takes zero days to investigate

Oct/Nov 2011

**111.** Identify the correct statement on the usage of Cyber Security Preparedness Indicators.

(A) They are used exclusively by the marketing department to advertise the bank's safety to new customers.
(B) They replace the need for Vulnerability Assessment and Penetration Testing in low-risk financial entities.
(C) They are applicable only to non-financial data assets stored in the bank's secondary off-site servers.
(D) They should be used for testing through independent compliance checks carried out by professionals.

May/June 2017

**112.** Consider the following statements and identify which describes the bank's responsibility under standard cyber resilience frameworks:

I To protect the confidentiality, integrity, and

Downloaded from www.pdf.tube

Oct/Nov 2014

**87.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option:
Assertion (A): Regulated Entities (REs) are advised to explore the feasibility of implementing code that checks if a device is rooted/jailbroken prior to the installation of the mobile application.
Reason (R): Rooted/jailbroken devices grant users super-user access, which can bypass the inherent security constraints of the operating system, posing a severe risk to payment applications.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation of Assertion (A).
(C) Assertion (A) is true, but Reason (R) is false.
(D) Assertion (A) is false, but Reason (R) is true.

May/June 2021

**88.** Consider the following actions required for fraud control staff and identify which are necessary:
I Set and update appropriate rules
II Monitor exceptions continuously and take prompt action
III Differentiate false positives from the rest
IV Communicate/escalate to appropriate authorities
V Conduct independent Penetration Testing of core systems
Which of the above statement(s) is/are correct?
(A) (I), (II), (III), and (IV)
(B) (II), (III), (IV), and (V)
(C) (I), (III), (IV), and (V)
(D) (I), (II), (IV), and (V)

Oct/Nov 2009

**89.** Consider the following security controls and identify which are mandated for mobile applications:
I Device policy enforcement
II Application sandbox/containerization
III Code obfuscation
IV Allowing unrestricted remote login access
Which of the above statement(s) is/are correct?
(A) (I), (II), and (III)
(B) (I), (III), and (IV)
(C) (II), (III), and (IV)
(D) (I), (II), and (IV)

May/June 2016

**90.** Identify the correct statement regarding the provision of digital payment products and services to a customer.
(A) Provide products only upon specific requisition with a positive acknowledgement of terms and conditions.
(B) They shall be provided automatically to all account holders upon account opening for banking convenience.
(C) Customers cannot opt out of digital payment services once they have successfully deposited initial funds.
(D) A verbal request over a standard phone call is sufficient to mandate activation of all digital services.

NODIA

Oct/Nov 2023

**91.** Consider the following actions and identify which are included in the scope of a standard cyber resilience framework:
I Appointment of a CISO
II Evolving a Cyber Crisis Management Plan (CCMP)
III Continuous surveillance via SOC
IV Relying solely on traditional BCP/DR arrangements
Which of the above statement(s) is/are correct?
(A) (I), (II), and (III)
(B) (I), (III), and (IV)
(C) (II), (III), and (IV)
(D) (I), (II), and (IV)

May/June 2011

**92.** The following question consists of two statements—Assertion (A) and Reason (R). Answer the question by selecting the appropriate option:
Assertion (A): Regulated Entities (REs) shall redact/mask sensitive customer information when transmitted via SMS/e-mails.
Reason (R): Transmission via SMS/e-mail occurs over clear channels which can be intercepted, hence masking preserves data confidentiality.
(A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
(B) Both Assertion (A) and Reason (R) are true, but Reason (R) is not the correct explanation

(C) P-4, Q-3, R-2, S-1
(D) P-3, Q-4, R-1, S-2

**Oct/Nov 2016**

**119.** Match the items in List I with those in List II:
List I: (Entity/Committee)
P. G Gopalakrishna Committee
Q. CERT-In
R. IDRBT
S. CSITE Cell
List II: (Attribute or Action)
1. Created under the Department of Banking Supervision (DBS)
2. Issued 2011 guidelines on Information Security and Cyber Frauds
3. Coordinates the CISOs' Forum
4. Government entity providing proactive and reactive cyber security services
(A) P-2, Q-4, R-3, S-1
(B) P-4, Q-2, R-1, S-3
(C) P-1, Q-3, R-2, S-4
(D) P-3, Q-1, R-4, S-2

**May/June 2023**

**120.** A bank has established a robust IT policy but lacks a dedicated Security Operations Centre (SOC). They argue that their annual external audits are sufficient for surveillance. How does the standard regulatory framework evaluate this stance?
(A) It is unacceptable as a SOC must be set up at the earliest to ensure continuous surveillance and monitoring.
(B) It is acceptable as long as the bank is classified as a low-risk entity by its primary regulator.
(C) It is acceptable if the IT Sub Committee approves the waiver based on the current financial year.
(D) It is unacceptable solely because external auditors cannot issue digital certificates to the bank.

**Oct/Nov 2008**

**121.** An executive receives a phone call from someone claiming to be from the IT department, asking for their password to perform a system upgrade. This type of social engineering attack is an example of Vishing. Once the executive realizes the deception and alerts the security team, which aspect of the CCMP is primarily activated?
(A) Prevention
(B) Archival
(C) Redaction
(D) Detection and Response

**May/June 2010**

**122.** Which of the following best defines the primary focus of Information Security as distinguished from Cyber Security?
(A) The ability to protect or defend the use of cyberspace from cyberattacks through proactive defenses.
(B) Protecting the confidentiality, integrity, and availability of information assets.
(C) Addressing risks emanating from cyber warfare and interconnected internet of things devices.
(D) Managing negative social impacts and risks from the interaction of people on the internet.

**Oct/Nov 2013**

**123.** Which of the following evaluations of digital security statements is incorrect?
(A) The evaluation of the statement "Customer is solely responsible for the security of his digital transactions" as False.
(B) The evaluation of the statement "'Device binding' is one of the mobile applications controls" as True.
(C) The evaluation of the statement "Data in transmission need to be safeguarded but data at rest need not be" as True.
(D) The evaluation of the statement "Data in transmission need to be safeguarded but data at rest need not be" as False.

**May/June 2008**

**124.** What is the definition of Cyberspace in the context of Cyber Security?
(A) Interconnected networks of information systems, infrastructures, the Internet, and computer systems.
(B) A localized environment designed solely for secure banking transactions and encrypted financial data.
(C) An isolated intranet facilitating internal communication within a bank and its branches.
(D) A regulatory sandbox environment for testing new digital payment applications and system logic.

Click Here to Buy book on Amazon

**Oct/Nov 2007**

**125.** What is the most appropriate statement summarizing the main objective of the Master Directions on Digital Payment Security Controls?

(A) To completely eliminate the use of physical cash in the national economy and move to digital credit.

(B) To mandate digital payment security controls to protect consumers against fraud in the digital space.

(C) To transfer the cost of digital payment infrastructure and maintenance to third-party technology vendors.

(D) To establish a single state-owned provider of digital payment applications for all commercial banks.

www.nodia.in

NODIA

# ANSWERS

1. (C) (II), (IV), (I), (III)
Regulatory developments began with the G. Gopalakrishna Committee recommendations in 2011. Subsequently, banks were instructed to communicate their board-approved Cyber Security Policy to the CSITE Cell by June 2016. Following this, Chief Information Security Officers had to report gaps and viable remediation plans by July 2016. Finally, the Master Directions on Digital Payment Security Controls were implemented.

2. (C) CERT-In
The Computer Emergency Response Team - India serves as the national nodal agency for responding to computer security incidents. It provides essential proactive and reactive services, including threat intelligence and assessment guidelines. This government entity plays a pivotal role in strengthening cyber security across various sectors by issuing timely alerts and advisories to mitigate digital vulnerabilities.

3. (C) Reserve Bank Information Technology Pvt. Ltd. (ReBIT)
The Reserve Bank of India established this specialized subsidiary to address the evolving technological and cyber security needs of the financial sector. Its primary mission involves ensuring the cyber resilience of Indian banking institutions. It focuses on research, innovation, and providing technical support to the central bank while monitoring emerging digital threats and improving defense mechanisms.

4. (C) It facilitates collective threat intelligence and the adoption of proactive cyber security measures.
Participating in collaborative platforms like the CISOs' Forum and the Indian Banks – Center for Analysis of Risks and Threats allows financial institutions to share vital security information. This cooperation enhances collective threat intelligence, enabling banks to adopt proactive measures against common vulnerabilities. It fosters a unified defense strategy and encourages the exchange of industry best practices.

5. (B) To highlight specific cyber risks and the corresponding measures required to mitigate these threats.
Maintaining a distinct Cyber Security Policy is essential because cyber threats are more dynamic and sophisticated than traditional information security risks. This separation allows financial institutions to clearly define specific vulnerabilities related to cyberspace. It ensures that the board-approved strategy focuses on specialized defense mechanisms, incident response plans, and mitigation techniques tailored to the digital banking environment.

6. (B) Only (II)
The supervisory reporting framework established by the regulator mandates a comprehensive approach to monitoring security events. It requires financial institutions to collect and report both summary-level information and detailed data concerning information security incidents. This dual reporting structure ensures that authorities have access to a complete overview of the threat landscape while facilitating in-depth analysis of specific breaches.

7. (B) Protecting the confidentiality, integrity, and availability of information assets.
Information security focuses broadly on safeguarding data assets from unauthorized access, use, or destruction. It centers on three core principles: maintaining the confidentiality of sensitive data, ensuring the integrity of information, and providing continuous availability for authorized users. While cyber security specifically addresses threats within the digital cyberspace environment, information security covers the overall protection of all information formats.

8. (A) Only (I) and (II)
Securing networks and databases is a critical responsibility that cannot be entirely delegated to external vendors. Unauthorized access must be strictly disallowed to protect sensitive data. Often, temporary connections remain open due to oversight, creating significant vulnerabilities.

Downloaded from www.pdf.tube

**41.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
For digital payment applications licensed from third-party vendors, Regulated Entities are required to establish an escrow arrangement for the source code. This is a critical risk management step that ensures service continuity. If the vendor defaults or becomes unable to provide support, the bank can access the source code. This safeguard protects the bank from operational disruptions and technical obsolescence.

**42.** (C) Board members can be held liable if they fail to establish due diligence in addressing cyber security.
The Board of Directors holds ultimate responsibility for the organization's security posture. They cannot delegate away their liability entirely to technical staff. Board members can be held directly liable for operational cyber losses if it is determined that they failed to establish due diligence. This includes tasks such as reviewing risk reports, allocating adequate resources, and ensuring a robust policy framework is in place.

**43.** (B) To assess whether digital payment services meet the required operational and security standards.
Key Performance Indicators and monitoring systems are established by senior management to evaluate the health of digital payment services. These tools allow the bank to track whether its applications meet both operational efficiency and mandated security standards. By monitoring performance metrics, the board can identify areas where security may be lagging and ensure that the digital ecosystem remains resilient against threats.

**44.** (D) (I), (II), and (III)
A policy for digital payment products must cover functionality, security, and performance. This includes ensuring that products are built securely from the outset and that there is adequate capacity for future expansion. Additionally, maintaining high availability is crucial for minimizing customer service disruptions. Mandatory physical visits for activation are not typically part of these digital-first requirements, as they may hinder user accessibility.

**45.** (C) Digital certificates used in the digital payment ecosystem must be renewed well in time.
Effective security management requires that digital certificates used for authentication and encryption be renewed well before their expiration date. This ensures continuous trust and security within the payment ecosystem. Additionally, applications must employ robust logging and monitoring to track user activity and detect anomalous behavior. Relying on outdated certificates or failing to monitor transactions can expose the bank to significant cyber risks.

**46.** (B) (I), (III), (IV), (V)
A comprehensive Cyber Crisis Management Plan is designed to provide a structured response to digital incidents. It must explicitly address four key areas: detection, response, recovery, and containment. By integrating these components, a bank ensures it can identify threats quickly, take immediate action to limit damage, restore affected services, and isolate compromised systems to prevent the further spread of an attack.

**47.** (B) Storing unencrypted customer passwords in client-side cookies for session continuity
Standard security controls for digital payment channels mandate the use of secure communication protocols and appropriate encryption levels. Implementing Web Application Firewalls is also a requirement to defend against online threats. However, storing unencrypted customer passwords in client-side storage like cookies is strictly prohibited. Such a practice would severely compromise data integrity and confidentiality, making the information easily accessible to malicious actors.

**48.** (B) Within 2 to 6 hours
Rapid communication is vital when a cyber-security incident occurs. The regulator requires all financial institutions to report any unusual cyber events within a tight window of two to six hours after detection. This prompt reporting allows for a coordinated response and helps authorities monitor the systemic risk levels across the entire banking sector, enabling other institutions to take defensive measures.

NODIA

global Internet, telecommunications systems, and embedded computer processors. Understanding this broad scope is essential for banks as they develop strategies to protect their digital assets and customer data from sophisticated attacks originating within this global network.

**17.** (D) Assertion (A) is false, but Reason (R) is true.
Banks have historically shown hesitation in sharing details about the cyber-incidents they face due to reputational concerns. However, the regulatory stance is that collaboration and information sharing are highly encouraged. By exchanging data on threats and best practices through forums like IB-CART, institutions can collectively strengthen their defenses. Sharing vulnerabilities does not inherently increase risk but rather enhances systemic resilience.

**18.** (A) Banks should immediately implement a Board-approved cyber-security policy and strategy.
Every bank is required to promptly implement a comprehensive cyber-security policy and strategy that has been formally approved by its Board of Directors. This policy must address the unique risks the institution faces based on its size and technological adoption. It serves as the foundation for the bank's digital defense mechanisms, ensuring that security measures are prioritized at the highest level.

**19.** (B) (I), (III), (IV), (V)
A robust Cyber Crisis Management Plan must explicitly address four critical pillars to ensure operational resilience during a security event. These mandated aspects are detection, response, recovery, and containment. By focusing on these specific areas, financial institutions can effectively identify breaches, take immediate action to mitigate impact, restore essential services, and prevent the further spread of the threat across their networks.

**20.** (A) Record the risk and cost trade-off decisions in writing for future supervisory assessment.
When a bank's IT Sub Committee evaluates security upgrades, they may face difficult decisions regarding costs and risks. Regulatory guidelines require that such trade-offs be clearly documented in writing. Recording the reasoning behind choosing a specific security measure ensures transparency and accountability. This documentation is essential for future supervisory assessments, allowing regulators to understand the bank's risk appetite and decision-making process.

**21.** (C) Failure to arrange for security concern escalation to appropriate levels for enabling quick action.
A critical component of an effective cyber security framework is the establishment of clear escalation paths. When technical staff detect sophisticated threats, there must be a defined mechanism to bring these concerns to the attention of senior decision-makers immediately. Failing to provide this structural link prevents the organization from taking swift action, thereby increasing the risk of a successful breach.

**22.** (A) Only (I)
The G. Gopalakrishna Committee provided the foundational guidelines on Information Security and Cyber Frauds via a circular issued on April 29, 2011. While these recommendations were comprehensive, they were not intended to be static. Security measures must remain dynamic and adaptive to keep pace with the rapidly evolving nature of technology and cyber threats, ensuring that banks maintain robust defenses.

**23.** (B) P-1, Q-4, R-2, S-3
Inherent risk levels dictate the depth of controls required for a bank's digital infrastructure. A low risk level requires baseline preventive controls, while moderate risk necessitates periodic vulnerability testing. High risk levels demand elevated monitoring capabilities to detect sophisticated threats. Finally, a very high risk categorization requires a highly adaptive incident response framework to manage the severe threats associated with complex environments.

**24.** (A) (I), (II), IV), and (V)
Cyber security preparedness is measured by developing indicators that assess the adequacy of the resilience framework. These indicators are used for comprehensive testing through independent compliance checks and audits. It is critical that these audits are conducted by qualified professionals, not just internal IT staff. Furthermore, assessing stakeholder awareness

Click Here to Buy book on Amazon

essential for signing and creating message digests, while digital certificates must be renewed on time to maintain trust. Logging and monitoring functions are critical for tracking user activity and identifying anomalous behavior within applications. Together, these elements form a comprehensive cryptographic framework that protects sensitive digital payment data from unauthorized access.

**58.** (A) Yes, because Scheduled Commercial Banks excluding RRBs are specified under the applicability clause.
The Master Directions on Digital Payment Security Controls define their scope by listing specific types of financial institutions. Scheduled Commercial Banks are included, but Regional Rural Banks are explicitly excluded from this particular set of requirements. Therefore, an RRB's interpretation that it is not mandated to follow these specific directions is correct based on the current regulatory applicability criteria defined in the document.

**59.** (A) Only (I)
Regulated Entities are required to periodically test their backed-up data and applications to ensure they can recover without losing transactions or audit trails. This is a vital component of operational resilience. However, the mandated frequency for these tests is generally half-yearly rather than quarterly. Regular testing verifies that the backup systems are reliable and ready to be used if a primary system fails.

**60.** (B) The Board and Senior Management are responsible for implementation and must review the policy yearly.
The governance of security risks requires high-level oversight and accountability. The Board and Senior Management are responsible for the implementation of digital payment policies and must review them at least on an annual basis. This ensures that the bank's security strategy remains current and effective. They cannot delegate this responsibility solely to technical staff or third-party providers, as they remain accountable.

**61.** (C) The adoption of Adaptive Authentication factors depending on user risk profile and behaviour
When a system detects a transaction from an unfamiliar location or suspicious behavior, it may trigger additional verification steps. This is known as adaptive authentication. By evaluating the risk profile of each request, the bank can dynamically adjust security requirements. This approach helps protect against unauthorized access while minimizing friction for legitimate transactions, ensuring that higher-risk activities undergo more rigorous authentication procedures.

**62.** (A) To ensure customers recognize legitimate interfaces and mitigate phishing risks during authentication.
Maintaining a uniform look and feel for internet banking sites, even when accessed through external portals, is a crucial security measure. It helps customers easily recognize legitimate interfaces and distinguish them from fraudulent sites. This consistency is vital for mitigating phishing risks during the authentication process. If the interface is familiar, users are more likely to notice anomalies that could indicate a malicious site.

**63.** (A) Thoroughly testing functionality and security controls before moving to the production environment.
Before launching any new digital payment service, a bank must conduct thorough testing of both functionality and security controls. This ensures that the application behaves as expected and that its protective measures are effective in a real-world environment. Moving a service to production without these evaluations is a significant violation of security requirements, as it exposes the bank and customers to risks.

**64.** (C) Securely wipe sensitive customer information from memory when the user exits the mobile application.
To protect customer privacy and security, mobile applications must handle sensitive data carefully. A key requirement is to securely wipe such information from the device's memory as soon as the user exits the application. Storing user IDs, passwords, or other sensitive details permanently on the device is prohibited. This practice prevents

NODIA

remains legally and regulatorily accountable for any data confidentiality breaches that may occur.

**33.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Under the Information Technology Act, banks are categorized as data owners and have a fundamental duty to protect information assets. They cannot avoid liability for security failures by claiming they are merely intermediaries. Since the responsibility for data confidentiality, integrity, and availability rests with the bank, it must implement robust controls. Failure to do so can result in legal consequences.

**34.** (B) Distributed Denial of Service (DDoS) mitigation techniques
To protect digital payment products from attacks that use overwhelming traffic to disrupt services, banks must implement specialized mitigation techniques. These tools are designed to detect and filter out malicious traffic spikes while allowing legitimate customer transactions to proceed. Using such defenses is critical for maintaining the availability of internet-based financial services and ensuring that systems remain resilient during targeted attacks.

**35.** (A) Regulated Entities (REs)
The Master Directions on Digital Payment Security Controls apply to a specific group of financial institutions collectively known as Regulated Entities. This term includes various organizations such as scheduled commercial banks, small finance banks, payments banks, and credit card-issuing non-banking financial companies. These entities must adhere to the mandated security standards to protect the integrity of the digital payment ecosystem and safeguard customers.

**36.** (A) No, REs partnering to co-develop applications must incorporate a threat modelling approach.
When Regulated Entities partner with fintech firms to co-develop digital applications, they must adhere to strict security life cycle requirements. This includes incorporating a comprehensive threat modelling approach during the development phase. Bypassing this step to speed up product rollout is not permitted. Threat modelling is essential for identifying potential vulnerabilities early, ensuring that the application is secure by design before launch.

**37.** (A) If the bank fails to create awareness, the stakeholder is not held responsible for resulting incidents.
Banks have a significant responsibility to educate their stakeholders about cyber-security risks and safe practices. If a bank fails to provide adequate awareness programs, the stakeholder may not be held responsible for security incidents that result from this lack of knowledge. Therefore, it is essential for financial institutions to conduct regular educational campaigns to ensure that employees and customers understand their roles.

**38.** (A) P-1, Q-2, R-3, S-4
Capacity building ensures that systems can meet growth demands and process transactions efficiently. High availability is necessary to minimize technical declines and maintain service continuity. A robust dispute resolution mechanism is essential for handling customer grievances effectively. Furthermore, the overall system architecture must be robust enough to handle increasing transaction volumes and customer growth while maintaining high security and performance levels.

NODIA

**39.** (C) Half-yearly
To ensure that digital payment products and services can be recovered without loss of data or audit trails, banks must periodically test their backup facilities. The mandated minimum frequency for testing backed-up data and applications is half-yearly. This regular testing ensures that the recovery systems are functional and capable of restoring operations quickly in the event of a system failure or breach.

**40.** (B) (II), (III), (I), (IV)
The regulatory timeline began with the first issuance of Cyber Security Guidelines. This was followed by a revision based on the Gopalakrishna Committee recommendations. Later, the specific Cyber Security Framework for Banks was notified. The final event in this sequence was the deadline for Chief Information Security Officers to report identified gaps and submit a viable remediation plan to the central bank.

Therefore, financial institutions must maintain direct oversight and implement robust internal controls to manage these risks and prevent potential security breaches.

**9.** (A) P-2, Q-1, R-4, S-3
Vishing is a voice-based phishing technique used to extract data, while Distributed Denial of Service attacks overwhelm system resources. Whaling specifically targets high-ranking senior executives with deceptive messages. Drive-by downloads involve the unintended execution of malware from compromised websites. Each of these threats requires distinct defensive strategies to ensure the overall security and resilience of digital banking infrastructures.

**10.** (C) It is prohibited as the Cyber Security Policy must be distinct from the broader IT policy framework.
Regulatory guidelines explicitly state that every bank must formulate a Cyber Security Policy that is separate from its broader Information Technology or Information Security policies. This ensures that the specific risks associated with cyberspace receive focused attention and dedicated resources. Merging these documents is not permitted because it may dilute the specialized strategies required to address digital threats.

**11.** (D) Ensure they are brought up to speed on cyber-security aspects and organize appropriate familiarization.
Banks must proactively educate their top management and board members regarding the critical aspects of cyber security. It is essential to organize familiarization sessions that help leadership understand emerging threats and their potential impact on operations. This high-level awareness ensures that the board can effectively oversee the implementation of security frameworks and allocate necessary resources for institutional resilience.

**12.** (D) Assertion (A) is false, but Reason (R) is true.
Modern technologies and digital tools significantly increase an organization's exposure to new vulnerabilities, necessitating advanced protective measures. However, the regulatory framework specifies that traditional information security issues and emerging cyber threats should be treated through distinct strategies. A unified framework is considered insufficient because cyber risks are highly dynamic and require a dedicated policy that is separate from IT.

**13.** (A) A Board-approved strategy addressing Detection, Response, Recovery, and Containment of cyber-risks.
A Cyber Crisis Management Plan is a comprehensive, board-approved strategy designed to handle severe digital incidents. It specifically addresses four vital operational areas: the detection of threats, the immediate response to incidents, the recovery of affected systems, and the containment of the breach. This plan goes beyond traditional business continuity measures by focusing on technical and operational resilience against cyberspace.

**14.** (C) Cyber-attacks are predictable and generally follow patterns that can be fully anticipated.
Continuous surveillance is a mandatory requirement for banks, often achieved through a dedicated Security Operations Centre. While vulnerability testing and regular updates are essential, it is incorrect to believe that cyber-attacks are entirely predictable. Threats constantly evolve with new techniques, meaning they cannot be fully anticipated. Constant monitoring and proactive threat intelligence are necessary to defend against these unpredictable digital events.

**15.** (D) Only successful cyber-attacks that result in financial loss need to be reported.
Regulatory guidelines require banks to report all unusual cyber-security incidents, regardless of whether they resulted in financial loss. This includes unsuccessful attempts that were detected but did not fructify. Providing a complete picture of the threat landscape is vital for systemic stability. All incidents must be reported to the regulator within a strict timeframe of two to six hours.

**16.** (A) Interconnected networks of information systems, infrastructures, the Internet, and computer systems.
In the context of cyber security, cyberspace refers to the complex and interconnected environment formed by digital networks. This includes various information systems, physical infrastructures, the

Downloaded from www.pdf.tube

**49.** (A) Failure to evaluate technology platform risks on both the server side and the client side.
Before launching a new digital payment service, banks are required to conduct a thorough risk evaluation of the technology platform. This assessment must cover both the server-side infrastructure and the client-side application architecture. Skipping these steps to meet launch deadlines represents a critical security failure. Neglecting to identify vulnerabilities on either side can expose both the bank's internal systems and customer devices.

**50.** (A) (I), (II), (III), and (IV)
To meet functionality, security, and performance standards, banks must implement several critical controls. These include protecting data confidentiality, establishing effective dispute resolution mechanisms, and ensuring swift corrective actions through review. Additionally, providing the necessary infrastructure and human resources is essential. However, permitting anonymous transactions is generally not a requirement for standard digital payment products, as it may conflict with security and accountability.

**51.** (A) Only (I) and (II)
The Application Security Life Cycle requires a 'secure by design' approach, where security is embedded during development rather than added later. Regulated Entities must also implement a multi-tier architecture to segregate application, database, and presentation layers for better isolation. Retroactively applying security after a product launch is not acceptable, as it leaves the application vulnerable during its most critical initial phase.

**52.** (D) They are held directly liable due to their failure to establish due diligence in the risk review.
In the event of a major security breach, the Board of Directors can be held directly liable if they failed to perform their due diligence. This includes neglecting to review gap reports from the CISO or failing to allocate necessary resources for cyber security. Regulatory frameworks emphasize that leadership must take an active role in risk oversight and cannot simply blame technical departments.

**53.** (C) Regional Rural Banks
The Master Directions on Digital Payment Security Controls specifically target a range of financial institutions, including payments banks, small finance banks, and credit card-issuing non-banking financial companies. These directions are part of a broader effort to secure the digital payment ecosystem. However, Regional Rural Banks are currently not included in the list of entities mandated to comply with these specific security controls.

**54.** (C) To avoid any compromise in the integrity of the data
Mandating that web applications avoid storing sensitive information in cookies or hidden HTML fields is a critical security measure. The primary goal is to prevent any compromise in the integrity and confidentiality of customer data. Information stored on the client side is easily accessible and can be manipulated by attackers. Keeping such data on secure servers ensures it remains protected from unauthorized tampering.

**55.** (A) They shall review the policy at least once every three years.
The Board and Senior Management are responsible for formulating and implementing policies for digital payment products. They must also ensure that effective performance monitoring systems are in place. However, the requirement for reviewing these policies is more frequent than once every three years. Regular periodic reviews are necessary to ensure that security measures remain effective against the rapidly changing landscape of cyber threats.

NODIA

**56.** (A) Sections 43, 43A - Payment Card Industry Data Security Standards (PCI-DSS)
Sections 43 and 43A are specific provisions of the Information Technology Act that deal with penalties and compensation for unauthorized access or failure to protect sensitive data. They are not the same as PCI-DSS, which is a global industry standard for card data security. While both are related to security, they belong to different legal and regulatory frameworks for protecting information.

**57.** (A) P-3, Q-1, R-2, S-4
Strong security relies on appropriate key lengths for encryption and hashing. Algorithms are

communication channels are often unencrypted and can be intercepted by third parties. By masking the information, banks prevent the exposure of sensitive data, thereby reducing the risk of misuse. This ensures that customers receive necessary notifications without compromising the confidentiality of their data.

**73.** (D) Passwords generated and dispatched by the Regulated Entity (RE) must possess unlimited validity.
Internet banking security controls require automatic session termination after inactivity and uniform authentication procedures. While web applications are vulnerable to various attacks, it is incorrect to say that passwords should have unlimited validity. On the contrary, passwords generated by the bank must be valid for only a limited period to enhance security. This practice minimizes the window of opportunity for attackers to use intercepted credentials.

**74.** (A) Only (I)
Regulated entities are mandated to establish effective systems for online dispute resolution as part of customer protection. However, it is incorrect to educate customers to download applications from any third-party website. On the contrary, banks must instruct users to download apps only from authorized and official sources. This precaution is essential to prevent the installation of malicious software that could compromise the user's device and data.

**75.** (D) Implementing alternatives to SMS-based OTP authentication mechanisms.
When both the mobile application and the SMS-based OTP reside on the same device, the security of the second factor may be weakened. In such cases, banks are advised to explore alternative authentication mechanisms. These could include in-app notifications or other secure methods that do not rely solely on SMS. This approach enhances security by ensuring that authentication factors are truly independent and more difficult for attackers to intercept.

**76.** (A) (I), (II), and (IV)
While Vulnerability Assessment and Penetration Testing are conducted at regular intervals, certain events trigger the need for immediate testing. These include the introduction of new IT infrastructure or digital payment applications. Additionally, any major change to existing systems or applications requires comprehensive testing. Minor cosmetic updates to a website's frontend typically do not necessitate a full round of VAPT unless they affect underlying security features.

**77.** (D) Deactivate older versions within six months of the release of a newer version in a timely manner.
To ensure all users are on a secure platform, Regulated Entities must manage mobile application versions proactively. They are required to deactivate older versions within a maximum of six months after a newer version is released. This timely phase-out ensures that users utilize the most secure and up-to-date features. Verifying the application version before allowing transactions is also a mandated practice to prevent the use of outdated apps.

**78.** (D) Block access after a set number of attempts, notify the customer, and use a secure re-activation process.
Banks must implement controls to thwart brute force attacks by limiting failed log-in attempts. After a predetermined number of unsuccessful tries, the system should automatically block access to the account. The customer should then be notified of the block. To restore access, the bank must use a secure and verified re-activation process. This approach balances security with user access and prevents automated software from guessing passwords.

**79.** (B) Direct the customer to remove the current application and proceed with the installation of a new copy.
If a mobile payment application detects a significant anomaly that could indicate a security compromise, the bank should take immediate action. The recommended response is to direct the customer to uninstall the current version and install a fresh, secure copy. This ensures that any potential malware or corruption is removed. It is a proactive step that protects the user's data and the integrity of the banking system.

Click Here to Buy book on Amazon

unauthorized access to data if the device is lost or stolen.

**65.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Implementing a real-time or near-real-time reconciliation framework is essential for the security of digital payment transactions. By reconciling transaction data with settlement files within twenty-four hours, banks can quickly identify and address any discrepancies. This timely process facilitates the better detection and prevention of suspicious activities. Efficient reconciliation is a critical control that helps maintain the financial and operational integrity of the bank.

**66.** (A) Web content must be loaded even if errors are detected during SSL/TLS negotiation to ensure speed.
Mobile applications must prioritize security over speed during data transmission. It is incorrect to load web content if errors are detected during SSL or TLS negotiations, as this could indicate an insecure connection. Instead, the application should ensure device binding, host version checksums for verification, and require re-authentication after periods of inactivity. These measures protect users from Man-in-the-Middle attacks and unauthorized access.

**67.** (C) Vulnerability Assessment (VA) - Conducted at least on a half-yearly basis
Regular security testing is mandatory to identify and mitigate potential weaknesses in digital payment applications. Vulnerability Assessments must be conducted at least on a half-yearly basis. While Penetration Testing is also required, its frequency may differ. These scheduled tests ensure that the bank's defense mechanisms are regularly evaluated against the latest threats. Additional testing is required whenever major changes are made to systems.

**68.** (B) The requirement that clear communication and instructions be provided when new security features are added.
When banks introduce new security features, such as biometric authentication, they have a regulatory duty to provide clear communication and instructions to their customers. This ensures that users understand how to use the feature correctly and safely. Failing to provide this information can lead to user confusion and operational issues. Customer education is an essential component of the overall security framework for digital services.

**69.** (A) Maintaining all historical versions to ensure backward compatibility across all legacy devices.
Mandated mobile payment controls include secure download procedures, data encryption, and minimizing data collection. However, maintaining all historical versions for legacy devices is not a requirement. In fact, banks are often encouraged to phase out older versions to ensure that all users are on a secure and up-to-date platform. This helps eliminate vulnerabilities that may be present in outdated versions of the application.

**70.** (C) Advanced software programming for developing proprietary operating systems
Staff in the fraud control function must possess a range of specialized skills, including investigative techniques and customer education methods. They also need to be capable of liaising with law enforcement agencies when necessary. While technical knowledge is helpful, advanced software programming for developing proprietary operating systems is not listed as a required skill. Their focus is on monitoring, analyzing, and preventing fraudulent activities.

**71.** (A) P-2, Q-1, R-4, S-3
Implementing a Web Application Firewall helps defend against online threats, while PCI-DSS compliance ensures the security of payment card data. A Cyber Crisis Management Plan is necessary for addressing detection, response, recovery, and containment during incidents. Additionally, mobile applications must require re-authentication if they remain unused for a set period. Each of these measures addresses a specific security requirement mandated for regulated entities.

**72.** (B) To protect sensitive payment data from exposure and potential misuse during the transmission process.
Redacting or masking sensitive details like account and card numbers in SMS or emails is a critical data protection measure. These

NODIA

helps determine the overall level of institutional risk and preparedness against attacks.

**25.** (B) Data lifecycle - Suitable systems and processes need to be put in place by banks
Banks are responsible for safeguarding customer data throughout its entire lifecycle, from collection to disposal. This requires the implementation of suitable systems and processes that ensure data security at every stage. Maintaining confidentiality and integrity is mandatory, as banks cannot claim to be mere intermediaries to avoid liability. Protecting custodial information is a fundamental duty that involves robust technical and administrative controls.

**26.** (D) It has limited coverage of risks like cyber warfare, Internet of Things (IoT), and modern social trolling.
Traditional information security frameworks often struggle to address the complexities of the modern digital landscape. These older models frequently lack adequate coverage for emerging risks such as cyber warfare, the vulnerabilities of interconnected Internet of Things devices, and the impact of modern social trolling. As banking becomes increasingly digitized, these specialized threats require more adaptive and comprehensive strategies than traditional perimeter-based security.

**27.** (A) IDRBT
The Institute for Development and Research in Banking Technology established the Indian Banks – Center for Analysis of Risks and Threats. This center serves as a collaborative platform for the banking sector to share threat intelligence and best practices. By centralizing the analysis of cyber risks, it helps individual banks strengthen their security posture and respond more effectively to emerging digital challenges.

**28.** (A) Profitability of the delivery channels
When assessing inherent risks, banks must evaluate several critical factors, including the technologies adopted and alignment with business requirements. They also need to consider organizational culture and both internal and external threats. While these elements are vital for developing a secure framework, the profitability of delivery channels is not explicitly mentioned as a required factor for determining the cyber-security posture.

**29.** (C) Cross-site scripting vulnerabilities in non-financial public forums
A Cyber Crisis Management Plan must prepare banks to address significant threats like Distributed Denial of Service, ransomware, and targeted attacks such as spear phishing or whaling. These threats directly impact banking operations and customer security. However, vulnerabilities in non-financial public forums are generally considered outside the scope of a bank's CCMP, which focuses on risks directly affecting its own systems.

**30.** (D) To continuously monitor and manage cyber risks in real time
The primary purpose of a Security Operations Centre is to provide continuous, real-time surveillance of a bank's digital environment. It acts as a centralized hub where security professionals monitor for anomalies, manage potential threats, and respond to incidents as they occur. By maintaining constant vigilance, the SOC ensures that the institution can proactively defend against cyber-attacks and minimize operational disruptions.

**31.** (C) Outsourcing all cyber risk management tasks to the Computer Emergency Response Team - India (CERT-In).
Standard cyber security frameworks require banks to address network security, formulate crisis management plans, and protect custodial information. While institutions should collaborate with external bodies like CERT-In for threat intelligence and incident reporting, they cannot outsource their entire cyber risk management responsibility. Each bank must maintain internal accountability and implement its own defense mechanisms to ensure the confidentiality and integrity of data.

**32.** (C) Assertion (A) is true, but Reason (R) is false.
Regulated entities are required to implement strict oversight and monitoring for any third-party personnel who have access to their systems. This ensures that security standards are maintained despite the dependency on external providers. However, using third-party services does not absolve the bank of its responsibilities. The bank

Downloaded from www.pdf.tube

**80.** (D) Connectivity - Connecting exclusively via public open Wi-Fi for all financial transactions
Customer education must focus on safe digital habits, such as using authorized app sources and installing regular updates. However, advising customers to connect exclusively via public open Wi-Fi for financial transactions is incorrect and dangerous. Public Wi-Fi is often insecure and easily intercepted by attackers. Instead, users should be encouraged to use secure, private networks for banking activities to protect their sensitive information from theft.

**81.** (C) To warn of potential Man-in-the-Middle attacks or insecure connections, preventing compromised data.
Displaying certificate errors during SSL or TLS negotiations is a critical security warning for users. These errors can indicate that the connection is not secure or that a Man-in-the-Middle attack is attempting to intercept data. By alerting the user to issues like expired or unrecognised certificates, the bank helps prevent the compromise of sensitive information. This transparency ensures that users do not proceed with transactions over untrusted connections.

**82.** (A) A method to send notifications or prompt consumers to complete additional steps to verify identities when requests are deemed doubtful
Adaptive authentication is a dynamic security approach that adjusts verification requirements based on the risk level of a request. If a transaction appears doubtful or deviates from a user's normal behavior, the system prompts for additional verification steps. This helps ensure that only authorized users can access the account. It is an effective way to enhance security for high-risk activities without unnecessarily complicating legitimate, low-risk interactions.

**83.** (B) P-2, Q-1, R-4, S-3
Suspicious transactional behavior is identified through documented rules, while system alerts must be parameterized and monitored. Fraud analysis is conducted to determine why an incident occurred and how to prevent it in the future. It is also essential for staff to differentiate false positives from actual threats. This structured approach to fraud management ensures that banks can effectively identify and respond to various types of financial crimes.

**84.** (A) P-4, Q-2, R-3, S-1
Code obfuscation makes source code difficult to reverse engineer, while sandboxing isolates the application to protect it from others on the device. Remote access identification prevents login if screen-sharing apps are detected. The phase-out mechanism ensures that older versions of the app are deactivated within a six-month period. These technical controls work together to secure mobile banking applications and protect customer data from various types of digital attacks.

**85.** (C) Only (I) and (III)
Internet banking websites are susceptible to brute force attacks, making it necessary to implement login attempt limits. Securely delivering passwords that are valid for only a limited period is also a vital control. However, allowing an online session to remain active indefinitely is incorrect. Sessions must be automatically terminated after a period of inactivity to prevent unauthorized access if a user forgets to log out from their browser.

**86.** (B) Regulated Entities (REs) shall transmit complete, unredacted customer account numbers via SMS to ensure transparency.
Banks must actively monitor for non-genuine applications on app stores and ensure that their servers block transactions from unauthorized apps. However, it is incorrect to transmit complete, unredacted account numbers via SMS. Such a practice would expose sensitive information over an insecure channel. Instead, masking and redaction should be used to protect customer data during transmission while still providing necessary transaction alerts and operational updates.

**87.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Banks are encouraged to check if a device is rooted or jailbroken before allowing the installation of payment applications. These modifications grant super-user access, which bypasses the built-in security features of the mobile operating system. This environment poses a severe risk to the integrity of payment apps and the security of customer data. Restricting access on such compromised devices is a proactive measure to prevent potential breaches.

NODIA

helps prevent potential fraud from remaining unnoticed for extended periods.

**104.** (D) Cyberspace
Cyberspace is the term used to describe the complex, interconnected global network of digital infrastructures. It encompasses the Internet, telecommunications systems, and a wide variety of computer systems and embedded processors. For financial institutions, understanding the nature of cyberspace is fundamental, as it is the environment in which digital transactions occur and where cyber threats originate. Protecting assets within this vast network requires specialized and adaptive security strategies.

**105.** (A) P-4, Q-2, R-3, S-1
A Web Application Firewall defends sites against online threats, while Bring Your Own Device refers to using personal hardware for work. Distributed Denial of Service is an attack that overwhelms system resources. Finally, PCI-DSS stands for the global Payment Card Industry Data Security Standards. Understanding these terms is essential for professionals working within the digital security and regulatory framework of the modern banking and financial sectors.

**106.** (A) P-4, Q-1, R-3, S-2
To secure ATMs, disabling USB ports prevents the loading of malicious software. Anti-skimming solutions are critical for stopping the extraction of card data at the machine. Time-based admin access is used to restrict high-level privileges to specific windows, which helps mitigate insider risks. Point-to-point encryption (PCI-P2PE) ensures that card details are securely encrypted throughout the transaction process, providing a robust layer of defense at merchant terminals.

**107.** (A) Because the authentication request is deemed doubtful according to the security policy and risk assessment.
Adaptive authentication triggers extra verification steps when a log-in or transaction request appears doubtful based on risk assessments. Factors such as unusual locations or devices can flag a request for more rigorous identity checks. This approach helps the bank identify potential fraud while allowing normal, low-risk activities to proceed without interruption. It is a critical tool for balancing user experience with the high-security standards required for digital payments.

**108.** (D) (I), (II), (III), (IV), and (V)
Various technical terms are used within the cyber security framework for banks. BYOD stands for Bring Your Own Device, while FHDE refers to Full Hard Disk Encryption. VAPT is the process of Vulnerability Assessment and Penetration Testing. OEM stands for Original Equipment Manufacturer, and the CISO is the Chief Information Security Officer. Each of these concepts plays a specific and important role in the overall digital defense strategy.

**109.** (D) Presentation and database layers can be combined into a single layer to enhance transaction speed.
The Application Security Life Cycle mandates a multi-tier architecture to ensure security through segregation. Combining the presentation and database layers into a single unit is not permitted, as it would compromise the isolation of sensitive data. Instead, these layers must remain separate to prevent an attacker from gaining direct access to the database if the presentation layer is breached. A secure design always prioritizes data isolation over transaction speed.

**110.** (C) An emerging, unanticipated cyber-threat for which no patch currently exists
A zero-day attack refers to a cyber-threat that exploits a previously unknown vulnerability in software or hardware. Since the flaw is unanticipated, no patch or fix is available when the attack occurs. These threats are particularly dangerous because they bypass existing defenses. A Cyber Crisis Management Plan must include strategies for detecting and containing these emerging risks, ensuring the bank can remain resilient even when facing unknown vulnerabilities.

**111.** (D) They should be used for testing through independent compliance checks carried out by professionals.
Cyber security preparedness indicators are developed to evaluate the effectiveness of an institution's resilience framework. These indicators are used during independent compliance checks and audits performed by qualified professionals. They help measure the

Click Here to Buy book on Amazon

**96.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
The requirement for CISOs to report gaps by July 2016 was a pivotal step in strengthening the cyber security of banks. This reporting process forced institutions to take a critical look at their current state of affairs and allocate more resources to address vulnerabilities. It also necessitated the creation of viable remediation plans. This mandate ensured that security was prioritized and that specific steps were taken to close identified gaps.

**97.** (D) (I), (II), (III), (IV), and (V)
Improving the security of ATMs involves multiple measures, such as implementing BIOS passwords and disabling USB ports. It also requires anti-skimming solutions and whitelisting to prevent unauthorized software. Upgrading to supported operating systems and allowing only time-based admin access further strengthens the machines against both physical and digital threats. Each of these steps is essential for protecting the integrity of ATM transactions and safeguarding customer card data.

**98.** (A) Regulated Entities should provide a mechanism on their app for customers to mark transactions as fraudulent.
To enhance customer protection, banks should include a feature in their mobile applications that allows users to easily report fraudulent transactions. This direct reporting mechanism helps the bank take quick action to secure the account and investigate the incident. Providing such a tool is more efficient than requiring a physical branch visit and ensures that unauthorized activities are addressed as soon as they are detected by the user.

**99.** (A) P-4, Q-1, R-3, S-2
Disabling USB ports prevents unauthorized software execution, while anti-skimming solutions protect against the extraction of card data. Time-based admin access reduces insider threats by restricting maintenance privileges. Finally, validating against PCI-P2PE ensures that card details are protected through point-to-point encryption at terminals. Together, these measures form a comprehensive defense strategy for ATM and card-based payments, protecting both the machines and the sensitive data they process.

**100.** (C) Security
When developing digital payment products, it is essential to consider functionality, performance, and security. While focusing on high availability and minimal technical declines addresses performance, ignoring data encryption is a critical failure in the security angle. Ensuring that sensitive information is protected is a mandatory requirement that cannot be overlooked. A product must meet all three criteria to be considered robust and compliant with standard regulatory security guidelines.

**101.** (A) No, banks must set up and operationalize a SOC to monitor cyber risks and threats in real time.
Regulatory guidelines require all banks to establish and operationalize a Security Operations Centre for continuous, real-time surveillance of cyber threats. Relying on periodic third-party audits is not an acceptable substitute for this constant monitoring. The SOC provides the necessary oversight to detect and respond to incidents as they happen. Each bank is responsible for maintaining this capability to ensure the resilience of its digital infrastructure.

**102.** (A) Only (I)
The Master Directions on Digital Payment Security Controls were issued primarily to enhance customer protection as digital payments continue to proliferate. These directions are mandatory for all specified Regulated Entities, not optional guidelines. They establish a uniform set of standards to secure the digital space and mitigate the risk of fraud. By mandating these controls, the regulator aims to maintain public trust and ensure the safety of the financial system.

**103.** (B) 24 hours
A robust reconciliation framework is essential for managing the risks associated with high volumes of digital transactions. Regulated entities must ensure that transaction files are reconciled against settlement data in a timely manner. The maximum permissible delay for this process is twenty-four hours from the receipt of the settlement files. This timeframe allows for the efficient detection of discrepancies and

Downloaded from www.pdf.tube

**88.** (A) (I), (II), (III), and (IV)
Effective fraud control requires staff to set and update rules, monitor exceptions, and take prompt action on alerts. They must also be able to differentiate false positives from real threats and escalate concerns to the appropriate authorities. While conducting VAPT is a security requirement, it is typically managed by a different technical team. The fraud control function focuses specifically on identifying and preventing deceptive activities through monitoring and analysis.

**89.** (A) (I), (II), and (III)
Device policy enforcement, application sandboxing or containerization, and code obfuscation are essential security measures for protecting mobile applications and data. However, allowing unrestricted remote login access is not a secure practice, as it increases vulnerability to unauthorized access and cyberattacks, making statement (IV) incorrect.

**90.** (A) Provide products only upon specific requisition with a positive acknowledgement of terms and conditions.
Digital payment products should only be provided to customers who have specifically requested them. The bank must also obtain a positive acknowledgement of the relevant terms and conditions before activating the service. Automatically providing these services to all account holders is not recommended, as it could increase the risk of fraud. Ensuring that customers explicitly opt-in helps maintain security and ensures they are aware of their responsibilities.

**91.** (A) (I), (II), and (III)
A standard cyber resilience framework encompasses the appointment of a CISO, the formulation of a CCMP, and continuous surveillance through a SOC. These elements are designed to provide a comprehensive defense against digital threats. Relying solely on traditional BCP and DR arrangements is insufficient for modern cyber risks. A more specialized and proactive approach is required to handle the unique challenges of the digital environment and ensure institutional safety.

**92.** (A) Both Assertion (A) and Reason (R) are true, and Reason (R) is the correct explanation of Assertion (A).
Banks must redact or mask sensitive customer details when sending them via SMS or email. This is because these channels often use clear, unencrypted transmission methods that can be intercepted by third parties. Masking information like account and card numbers helps preserve data confidentiality and prevents misuse if the message is accessed by an unauthorized person. It is a vital control for protecting customer privacy during communications.

**93.** (C) Use of ATMs that have unsupported operating systems shall be prohibited.
Maintaining the security of ATMs requires the use of modern and supported operating systems. Regulated entities are prohibited from using ATMs that run on unsupported versions, as these systems no longer receive critical security patches. Using outdated software leaves the machine vulnerable to various attacks. Banks must ensure that all ATMs are regularly updated with the latest supported versions and security patches to protect customer transactions.

**94.** (C) A maximum number of failed log-in attempts set down after which access is blocked
Brute force attacks involve automated software trying many password combinations to gain unauthorized access. To thwart this specific threat, banks must implement a limit on the number of failed log-in attempts. Once this threshold is reached, the system should automatically block access to the account. This control is essential for preventing unauthorized users from successfully guessing passwords and ensures that the digital banking interface remains secure.

**95.** (B) It caters solely to the cyber security needs of foreign banks operating outside India.
ReBIT is an IT subsidiary of the Reserve Bank of India, created to address the technological and cyber security needs of the Indian banking sector. Its purpose is to ensure the cyber resilience of institutions operating within the country, not just foreign banks abroad. ReBIT focuses on research, monitoring threats, and providing technical support to strengthen the overall security posture of the national financial infrastructure.

NODIA

level of risk and the readiness of the bank to face cyber threats. By using these objective metrics, the board can gain a clearer understanding of the organization's overall security posture and identify areas for improvement.

**112.** (B) Only (I) and (III)
Under standard resilience frameworks, a bank's primary duty is to protect the confidentiality, integrity, and availability of its data assets. It is also responsible for creating cyber security awareness among all relevant stakeholders. However, a bank cannot claim to be a mere intermediary to avoid legal liability. As the data owner, the institution remains fully accountable for maintaining security and ensuring that appropriate controls are implemented across all its digital channels.

**113.** (C) Assertion (A) is true, but Reason (R) is false.
Regulated entities are required to have an escrow arrangement for the source code of third-party licensed payment applications. This measure is intended to ensure service continuity if the vendor is unable to provide support. However, the escrow agreement does not guarantee that the third party will continue to update the code with new features. Its primary purpose is to provide the bank with access to the existing code for maintenance and survival.

**114.** (B) To make the application's source code difficult for attackers to understand and reverse engineer.
Code obfuscation is a security technique used to protect mobile applications from unauthorized analysis. By modifying the source code to make it complex and difficult to follow, banks can deter attackers from understanding the application's logic. This makes it much harder for malicious actors to reverse engineer the app and find vulnerabilities. It is a vital technical control that adds an important layer of defense to sensitive digital payment services.

**115.** (C) Installing unsupported operating systems to obscure source code
Maintaining a secure ATM network requires several key actions, such as disabling auto-run features and applying the latest operating system patches. Implementing terminal security solutions is also essential. However, installing unsupported operating systems is not a requirement and is actually prohibited. Unsupported systems increase risk because they do not receive security updates. Security through obscurity is not a valid strategy; instead, banks must use modern, fully supported software to protect their machines.

**116.** (D) Disabling transaction limits at the Card and BIN level to ensure customer convenience
Effective surveillance of card transactions involves monitoring overseas withdrawals and setting rules based on the bank's risk appetite. It is also important to identify any unencrypted payment data within the ecosystem. However, disabling transaction limits is not a recommended practice for security. In fact, maintaining and monitoring these limits at various levels is essential for preventing large-scale fraud. Convenience should not come at the expense of necessary security controls.

**117.** (D) Online Dispute Resolution (ODR) systems are prohibited due to security concerns.
Banks are required to incorporate a clear section in their applications for lodging grievances, including forms and contact details. They must also adhere to regulatory instructions for resolving digital payment disputes. However, the statement that Online Dispute Resolution systems are prohibited is incorrect. On the contrary, banks are encouraged to implement ODR systems to provide customers with an efficient and accessible way to resolve issues related to their digital payment transactions.

**118.** (A) P-2, Q-1, R-4, S-3
A Web Application Firewall is used to protect against online threats, while PCI-DSS compliance is necessary for securing card data. A Cyber Crisis Management Plan must be formulated to cover detection, response, recovery, and containment. Additionally, mobile applications should require re-authentication after being unused for a designated period. Each of these mandated controls addresses a different aspect of the overall security framework required for digital payment products and services.

**119.** (A) P-2, Q-4, R-3, S-1
The G. Gopalakrishna Committee issued foundational guidelines in 2011, while CERT-In provides proactive and reactive cyber security

Click Here to Buy book on Amazon

services. IDRBT is responsible for coordinating the CISOs' Forum, helping banks share threat intelligence. The CSITE Cell was created under the Department of Banking Supervision to oversee cyber security and IT examinations. Each of these bodies plays a distinct role in shaping the regulatory and operational landscape of cyber security in Indian banking.

**120.** (A) It is unacceptable as a SOC must be set up at the earliest to ensure continuous surveillance and monitoring.
Regulatory guidelines are clear that having an IT policy and annual audits is not enough for modern security needs. Every bank is mandated to establish a dedicated Security Operations Centre at the earliest. The SOC is necessary for providing continuous, real-time surveillance of the bank's digital environment. Without this capability, an institution cannot effectively monitor for and respond to the rapidly evolving threats that characterize the current cyberspace landscape.

**121.** (D) Detection and Response
When a social engineering attack like vishing is identified by an employee, the bank must activate its crisis management procedures. Once the deception is realized and the security team is alerted, the detection and response aspects of the CCMP are primarily engaged. This involves identifying the threat and taking immediate steps to mitigate any damage. Such a proactive approach is essential for protecting sensitive information and maintaining the security of the organization's systems.

**122.** (B) Protecting the confidentiality, integrity, and availability of information assets.
Information security is a broad discipline focused on the protection of all data assets. Its primary goal is to ensure the confidentiality, integrity, and availability of information, whether it is in digital or physical form. While cyber security specifically addresses the defense of digital networks and cyberspace, information security covers the overall management of data risks. Understanding this core focus is essential for developing comprehensive strategies to safeguard a bank's valuable information resources.

**123.** (C) The evaluation of the statement "Data in transmission need to be safeguarded but data at rest need not be" as True.
In a robust security framework, all data must be protected, whether it is in transit or at rest. It is incorrect to believe that only transmitted data requires safeguarding. In fact, sensitive information stored on servers or devices is also a target for attackers and must be encrypted or otherwise secured. Therefore, an evaluation that claims data at rest does not need protection is false, as both states are equally vulnerable.

**124.** (A) Interconnected networks of information systems, infrastructures, the Internet, and computer systems.
Cyberspace is the comprehensive digital environment created by interconnected networks. This includes various information systems, physical and digital infrastructures, the global Internet, and embedded computer processors. For the banking sector, cyberspace is the critical medium through which digital payments and services are delivered. Recognizing the broad and interconnected nature of this environment is essential for developing effective cyber security policies and technical controls to protect institutional and customer assets from digital threats.

**125.** (B) To mandate digital payment security controls to protect consumers against fraud in the digital space.
The main objective of the Master Directions on Digital Payment Security Controls is to establish a secure environment for digital transactions. By mandating specific security measures for regulated entities, the regulator aims to protect consumers from fraud and misuse in the digital space. These controls are essential for maintaining public confidence in digital banking services as they become more widespread. Protecting the consumer is the central priority of this comprehensive regulatory framework.

NODIA

Visit :
www.pdf.tube

Download PDFs For :

- ✓ Chapterwise Question Bank
- ✓ JEE NEET Foundation
- ✓ Primary Classes Worksheets
- ✓ Olympiad Guide
- ✓ Sample Papers
- ✓ Previous Year Papers
- ✓ Previous JEE Papers
- ✓ Previous NEET Papers

Nodia Editions LLP
125, Sector 6, Vidhyadhar Nagar, Jaipur 302039

MRP ₹ 690.00

Downloaded from www.pdf.tube